

VERBATIM <sup>1</sup>RECORD OF TRIAL <sup>2</sup>

(and accompanying papers)

of

MANNING, Bradley E.

(Name: Last, First, Middle Initial)

Headquarters and  
Headquarters Company,  
United States Army Garrison  
(Unit/Command Name)

(Social Security Number)

U.S. Army

(Branch of Service)

PFC/E-3

(Rank)

Fort Myer, VA 22211

(Station or Ship)

By

GENERALCOURT-MARTIAL

Convened by

Commander

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

(Date or Dates of Trial)

## Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

<sup>1</sup> Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

<sup>2</sup> See inside back cover for instructions as to preparation and arrangement.

Tourists in Iceland don't Respect Obstructions

Little Italy in Reykjavik

Snowden on his way to Iceland?

Nature Reserve in Icelandic Highlands Extended

Anita Hinnksdottir with Icelandic record and a ticket Russia

[See more](#)



Be the first to find out. Our weekly massive announces new events, discounts and backstories

Name

Email

[Send](#)

**INSPIRED** Inspired by Iceland

**ICELAND** Like

81,292 people like Inspired by Iceland.



Facebook social plugin

[Sign Up](#)

Create an account or Log

In to see what your friends are doing.

INSPIRED ICELAND

## ICELAND.IS

Promote Iceland  
Sundagarðar 2  
104 Reykjavík  
Iceland  
Tel. 354 511 4000  
Fax. 354 511 4040

## OFFICIAL LINKS

Inspired by Iceland  
Invest in Iceland  
Visit Iceland  
Cruise Iceland  
Iceland Convention  
Be friends with Iceland

## ICELAND.IS

The Big Picture  
Arts & Culture  
Travel & Leisure  
Trade & Invest  
Iceland Abroad  
Press & Media

## STAY IN TOUCH

Email Iceland.is  
Email Invest.is  
Webmaster  
Recommend to a friend



GOVERNMENT OFFICES OF ICELAND

You are here: Home

## English

- Home
  - Current government
  - Government Offices
  - How Iceland is governed
- 

## Ministries

- Prime Minister's Office
- Ministry of Education, Science and Culture
- Ministry for the Environment and Natural Resources
- Ministry of Finance and Economic Affairs
- Ministry for Foreign Affairs
- Ministry of Industries and Innovation
- Ministry of the Interior
- Ministry of Welfare

## Institutions and Agencies

## News and Press Releases

17 Jun Prime Minister's Office  
Address by the Prime Minister, Mr Sigmundur Davíð Gunnlaugsson, at  
Austurvöllur, 17 June 2013



"We Icelanders wish to participate in international cooperation and to work with nations all over the world, sharing our experience, knowledge and strengths but at the same time learning from others and benefiting from their strengths."

#### **4 JunMinistry for Foreign Affairs**

##### **Embassy in Moscow takes over issuing of visas for Iceland**

Applications for visas continue to be received at the VFS Global service centres in St. Petersburg and Moscow.

#### **3 JunMinistry for Foreign Affairs**

##### **Political Advisor to the Minister**

Margrét Gísladóttir has been appointed as a Political Advisor to Gunnar Bragi Sveinsson, Minister for Foreign Affairs

31.5.2013**Prime Minister's Office** Prime Minister meets with President of Finland

29.5.2013**Ministry of Finance and Economic Affairs** Treasury Finances January-April 2013

23.5.2013**Ministry for Foreign Affairs** New Minister for Foreign Affairs

23.5.2013**Prime Minister's Office** New Icelandic Government takes office

22.5.2013**Ministry of Finance and Economic Affairs** Draft legislation on Financial Stability Council

20.5.2013**Ministry for Foreign Affairs** The Arctic States sign an agreement on Marine Oil Pollution Preparedness and Response

16.5.2013**Ministry for Foreign Affairs** Gender Equality Studies and Training Programme (GEST) Joins the UN University Network

6.5.2013**Ministry of the Interior** Application for Icelandic citizenship- New point of contact



MINISTRY FOR FOREIGN AFFAIRS

---

## Shortcuts

- Protocol Department
- Publications
- Consular Affairs
- EU Application
- Information on Iceland
- Diplomatic Missions
- VISA to Iceland
- Icesave
- Free Trade Agreement Iceland - China

## Enquiries

### Diplomatic Missions

## News from the Ministry

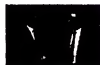
### **Electronic publication: Gender Equality in Iceland's Development Cooperation and Iceland's second NAP on implementing UNSCR 1325**

21 Jun

The Ministry for Foreign Affairs has published two new policy documents; Gender Equality in Iceland's Development Cooperation and a National Action Plan for the implementation of UNSCR 1325. Both documents are formulated in line with the Strategy for Iceland's Development Cooperation 2013-2016, where gender equality and women's empowerment is emphasised.

### **Minister Sveinsson meets with UK's Minister for Europe**

20 Jun



Foreign minister Gunnar Bragi Sveinsson met yesterday with UK's Minister for Europe, David Lidington. Minister Sveinsson explained the Icelandic Government's decision to put further accession negotiations with the European Union on hold, and what that entails. Mr. Lidington spoke of the current dialogue in the UK regarding the country's future relationship with the EU and the Government stand on the matter.

13.6.2013 **Minister Sveinsson meets with Stefan Füle**

13.6.2013 **Minister Sveinsson meets with the NATO Secretary General**

4.6.2013 **Embassy in Moscow takes over issuing of visas for Iceland**

**More news...**

**RSS-feed**

**More news...**



**Icelandic Ministry for  
Foreign Affairs**

Like 1,073

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

PROSECUTION MOTION  
FOR JUDICIAL NOTICE

Enclosure 12

24 June 2013



## Birgitta Jónsdóttir

Date of Birth: April 17th, 1967

Telephone: +354 5630 500

Homepage: [birgitta.is](http://birgitta.is)

E-mail: [birgittaj@althingi.is](mailto:birgittaj@althingi.is)

Party:

- Chairman of the Movement 2011-2012.

### Parliamentary Career

- Member of Althingi for the Reykjavik South Constituency 2009-2013 and for the Southwest Constituency since 2013.

### Party Group

- Chairman of the parliamentary group of the Pirate Party since 2013.
- Chairman of the parliamentary group of the Movement 2013 and 2009-2010.
- Vice-Chairman of the parliamentary group of the Movement 2012-2013 and 2010-2011.

### Present committees

- Member of the Constitutional and Supervisory Committee since 2013 (2nd Vice-Chairman since 2013).
- Observer in the Foreign Affairs Committee since 2011.
- Member of the Icelandic delegation to the Inter-Parliamentary Union (IPU) since 2013.
- Member of the EU-Iceland Joint Parliamentary Committee since 2010.
- 

### Earlier committees

- Member of the Judicial Affairs and Education Committee 2011-2013.
- Member of the Foreign Affairs Committee 2009-2011.
- Member of the Environment Committee 2009-2011.
- Member of the Special Committee on the Standing Orders of Althingi 2011-2013.
- Member of the Parliamentary Review Committee on the SIC report 2009-2010.
- Member of the Icelandic delegation to the NATO Parliamentary Assembly 2009-2013. Observer in the Foreign Affairs Committee's Working Group on European Affairs 2011-2013.

- Member of the Foreign Affairs Committee's Working Group on European Affairs 2010-2011.

---

©Secretariat of Alþingi  
[Contact us](#)



EMBASSY OF ICELAND  
MOSCOW

Home

Embassy Information

Ambassador

Personnel

Consulates

Embassy's Jurisdiction

News and Events

Bilateral Relations

Business and Trade

Cultural Affairs

Consular Services

Links

MINISTRY FOR FOREIGN AFFAIRS

OTHER EMBASSIES

ICELAND IS

РУССКИЙ

## Ambassador

### CURRICULUM VITAE

## Albert Jónsson



Albert Jónsson

Born 28 December 1952 in Reykjavík.

Married to Ása Baldvinsdóttir with two children, Baldvin (born 1983) and Auður (born 1989).

1978: B.A. History and Political Science, University of Iceland.

1979: M.Sc. International Relations, University of London (London School of Economics and Political Science).

1980-1982: Researcher, Icelandic Commission on Security and International Affairs.

1983-2006: External lecturer in International Politics, University of Iceland.

1984-1987: Radio journalist for Iceland Broadcasting Service.

1987-1988: Television journalist for Iceland Broadcasting Service.

1988-1991: Executive Director, Icelandic Commission on Security and International Affairs.

1991-2004: Foreign Policy Adviser to the Prime Minister.

2004-2006: Special Adviser to the Foreign Minister.

2006 (June-October): Foreign Policy Adviser to the Prime Minister.

2006-2009: Ambassador to the United States.

2009-2011: Consul General, Faroe Islands.

2011- Ambassador to the Russian Federation.

### GET E-MAIL UPDATES

Be the first to find out. Our newsletter provides all the latest news, information and events

Name

E-mail

Send

INSPIRED BY ICELAND

### EMBASSY OF ICELAND MOSCOW

115127 Moscow,  
Khlobovy pereulok 28  
Russian Federation  
Tel +7 (495) 956-7604  
Fax 7 495 956 76 12

icemb.moscow@utin.sfr.is  
iceland.is/ru

### OPENING HOURS

Monday-Friday  
09 00 - 17 00

### GET E-MAIL UPDATES

Be the first to find out. Our newsletter provides all the latest news, information and events

Name

E-mail

Send

### CONTACT US

Name

E-mail

Subject

Send



## Jóhanna Sigurðardóttir, Prime Minister 2009-2013



### Political and Parliamentary activities:

- Prime Minister of Iceland February 1st 2009 - May 23rd 2013.
- Minister of Social Affairs July 8th 1987–June 24th 1994 and May 24th 2007 – February 1st 2009.
- Member of Althingi (the Parliament) for the Reykjavík constituency 1978–2013.
- Member of Althingi's Presidium 1979, 1983–1984 and 2003–2007.
- Member of the Committee on Foreign Affairs 1995–1996, Committee on Industry 1995–1999, Althingi's Special Committee on Constitutional Affairs 1995–1997, 1999–2000 and 2004–2007, Committee on General Affairs 1996–1999, Committee on Economy and Trade 1999–2007, Committee on Credentials 1999–2003 and Committee of Social Affairs 2003–2007.
- Member of the Icelandic Delegation to the IPU 1996–2003.
- Member of the Icelandic Delegation to the OSCE Parliamentary Assembly 2003–2007.
- Vice Chairman of the Social Democratic Party 1984–1993.
- Leader of the Social Democratic Alliance 2009–2013
- Chairman of the Board of Governors on Issues concerning Mentally Challenged and Disabled Persons 1979–1983.
- Member of Committee preparing a Bill on the Arrangement and Implementation on Adult Education and Revision of the Social Security Act 1978.
- Member of the Board of Social Security 1978–1987, Chairman of the Board 1979–1980.
- Participant of Conventions of the Inter-Parliamentary Union (IPU) 1980–1985.
- Chairman of the political party Þjóðvaki, 1995.

Jóhanna Sigurðardóttir is born in 1942.

## **Jóhanna Sigurðardóttir's Speeches and Articles 2009 - 2013**

### **Address of the Prime Minister of Iceland at official ceremonies on the parliament square Austurvöllur, 17 June 2011**

17.6.2011

"It will take more than empty words to put Iceland back on its feet, it will take energy, thrift, foresight and persistence."

### **Article by the Prime Minister of Iceland regarding the referendum on 9 April, published in Guardian today**

13.4.2011

"In a referendum held last Saturday, the Icelandic people decided to reject a legislation providing a state guarantee for the reimbursement payments by the Icelandic Deposit Guarantee Fund to the governments of the United Kingdom and the Netherlands."

### **A speech by Jóhanna Sigurðardóttir, Prime Minister of Iceland on Íslendingadagurinn August 2nd 2010**

2.8.2010

"We have a very special bond between Iceland and Canada – made strong by common history and shared heritage."

### **A speech by Jóhanna Sigurðardóttir, Prime Minister of Iceland, 31 July 2010**

31.7.2010

"It is a great pleasure to stand here at this historic site - on the grounds of Borg in Mountain, North Dakota - and be with you as you honor the heritage and history of Iceland. A country far away but still in your hearts. I am touched and grateful to witness how dedicated you are to the land of your forefathers and how determined you are not to forget where your ancestors came from."

### **Prime Minister's Address to the Nation on 17 June 2010**

21.6.2010

"Today, on this beautiful summer's day, we celebrate our national holiday all across the country. We celebrate our independence and our joy at living our lives in this country, on our bountiful island."

### **From Rescue to Recovery**

14.10.2009

Prime Minister Jóhanna Sigurðardóttir wrote an article in The Banker Magazine the 5th of October 2009 about the future outlook one year after the economic crises hit Iceland with severe consequences.

### **Prime Minister's Address Opening the Parliamentary Session on Monday, 05 October 2009**

8.10.2009



Althingi reconvenes now following an unusually brief recess - in a year we will not soon forget. It has been a very difficult time for the nation, because all of us suffered a shock when so many things we trusted failed.

### **Prime Minister's Opening Address to the Icelandic parliament Althingi**

20.5.2009

Prime Minister's, Jóhanna Sigurðardóttir, Opening Address to the Summer Session of the Icelandic parliament Althingi, on Monday, 18 May 2009.

### **Excerpts from the address delivered by Prime Minister Jóhanna Sigurðardóttir at the AGM of the Central Bank of Iceland, on 17 April 2009**

21.4.2009

"Trust is a key word - not only during the economic downturn we are currently experiencing and in financial markets, but in all areas of society and in government. Trust is the foundation of all our relations, and the foundation of a healthy, everyday society."

### **Platform of the Government - Report from the Prime Minister**

6.2.2009

"It can have escaped no one that our country is passing through a deep economic downturn. Within a very brief period, the government has had to act responsibly and determinedly, to keep the wheels of business and industry turning and to reinforce the security net for the nation's households and families."

### **Jóhanna Sigurðardóttir, Prime Minister 2009-2013**

1.2.2009

---

POPULAR TOPICS

BROWSE EXPERTS (EXPERTS)

QUIZZES (QUIZ/BROWSE)

IMAGE GALLERIES (GALLERY/BROWSE)

LISTS (LIST/BROWSE)



Written by  
Michael Ray



QUIZ  
The Library  
World

Contribute to  
This Article



LIST  
9 Diagnoses  
by Chae's  
Octane



QUIZ  
European  
History Quiz



GALLERY  
World War I

## ENCYCLOPÆDIA BRITANNICA<sup>®</sup>

ADVOCACY FOR ANIMALS (HTTP://ADVOCACY.BRITANNICA.COM) | BLOG (HTTP://WWW.BRITANNICA.COM/BLOG) | HELP (HTTP://HELP.EB.COM/PRIMUWINDEX.HTM)  
SCHOOL & LIBRARY PRODUCTS (HTTP://INFO.EB.COM) | SHOP (HTTP://STORE.BRITANNICA.COM)  
LOGIN | SUBSCRIBE (HTTP://SAFE1.BRITANNICA.COM/REGISTRATIONS/SIGNUP.D07/PARTNERCODE=EBOPPOSUE)

### Jóhanna Sigurðardóttir

Article Free Pass

Introduction (EBchecked/topic/1511694/Johanna-Sigurardottir)

Related (related places/1511694/related places to Jóhanna-Sigurardottir)

Jóhanna Sigurðardóttir, (born Oct. 4, 1942, Reykjavík, Ice.), Icelandic politician who became prime minister of Iceland in 2009. She was the country's first female prime minister and the world's first openly gay head of government (EBchecked/topic/240105/government) (Per-Kristian Foss served briefly as acting prime minister of Norway in 2002).

#### IMAGES

View  
Print  
Email  
Share



Sigurðardóttir worked as a flight attendant for Loftleiðir Icelandic Airlines from 1962 to 1971, and she was an active labour union member, twice serving as chairman of the board of the Icelandic Cabin Crew Association (1966, 1969). She took an office (EBchecked/topic/425680/office) job in Reykjavík in 1971. While there she continued her association with organized labour, and she sat on the board of the Commercial Workers' Union. In 1978 Sigurðardóttir was elected to the Alþingi (parliament) as a member of the Social Democratic Party, representing Reykjavík. She quickly gained a reputation as an advocate for social justice, and she called for the strengthening of Iceland's welfare system. She was named minister of social affairs in 1987, a position she held until 1994, when she unsuccessfully campaigned for leadership of the Social Democratic Party. Sigurðardóttir responded to this setback by forming her own party, National Movement, which captured four seats in the subsequent parliamentary election. The two parties reconciled in 1999, when they joined with the Women's Alliance and the People's Alliance to contest that year's election; in 2000 the coalition formally became the Social Democratic Alliance.

By this time Sigurðardóttir had established herself as one of the leading personalities in Icelandic politics. She returned to the ministry of social affairs in 2007, and she emerged as a voice of calm in the wake of Iceland's financial collapse in 2008. After the resignation of conservative Prime Minister Geir Haarde in January 2009, Sigurðardóttir led a coalition of Social Democrats and Left-Greens to form a caretaker minority government. On Feb. 1, 2009, she was formally sworn in as Iceland's prime minister. In the April elections the Social Democrats and Left-Greens won 34 seats, capturing a slim majority in the 63-member parliament. Shortly thereafter Sigurðardóttir announced that one of her top priorities as prime minister would be securing Iceland's membership in the European Union.

On June 27, 2010, the day that same-sex marriage became legal in Iceland, Sigurðardóttir and her partner Jónína Leósdóttir were married by means of a simple conversion of their registered partnership.

#### PLACES TOPICS



Iceland



Reykjavík  
(Iceland)

Michael Ray (https://user-profile/6392)

Try Britannica Online Premium for \$  
(https://uk1.britannica.com/registration/signup-uk1-partnerCode=EBOP1PC7GDOR\_MDL)



Britannica Kids  
Information You Can Trust  
ACTIVATE MY FREE TRIAL  
(https://safe1.britannica.com/registrations/partnerCode=EBOK300X100)



#### QUIZZES



Science Quiz  
(/quiz/41/science-quiz)



History: Fact or  
Fiction?



Science: Fact or  
Fiction?

See More... (/quiz/browse/all)





## Former Ministers

- Mr. Össur Skarphéðinsson; February 2, 2009 - May 23, 2013
- Mrs. Ingibjörg Sólrún Gísladóttir; May 24, 2007 - February 1, 2009
- Mrs. Valgerður Sverrisdóttir; June 15, 2006 - May 24, 2007
- Mr. Geir H. Haarde; September 27, 2005 - June 15, 2006
- Mr. Davíð Oddsson; September 15, 2004 - September 27, 2005
- Mr. Halldór Ásgrímsson; May 23, 2003 - September 15, 2004
- Mr. Halldór Ásgrímsson; May 28, 1999 - May 23, 2003
- Mr. Halldór Ásgrímsson; April 23, 1995 - May 28, 1999
- Mr. Jón Baldvin Hannibalsson; April 30, 1991 - April 23, 1995
- Mr. Jón Baldvin Hannibalsson; September 10, 1989 - April 30, 1991
- Mr. Jón Baldvin Hannibalsson; September 28, 1988 - September 10, 1989
- Mr. Steingrímur Hermannsson; July 8, 1987 - September 28, 1988
- Mr. Matthías Á. Mathiesen; January 24, 1986 - July 8, 1987
- Mr. Geir Hallgrímsson; May 26, 1983 - January 24, 1986
- Mr. Ólafur Jóhannesson; February 8, 1980 - May 26, 1983
- Mr. Benedikt Gröndal; October 15, 1979 - February 8, 1980
- Mr. Benedikt Gröndal; September 1, 1978 - October 15, 1979
- Mr. Einar Ágústsson; August 28, 1974 - September 1, 1978
- Mr. Einar Ágústsson; July 14, 1971 - August 28, 1974
- Mr. Emil Jónsson; July 10, 1970 - July 14, 1971
- Mr. Emil Jónsson; August 31, 1965 - July 10, 1970

- Mr. Guðmundur Í. Guðmundsson; November 14, 1963 - August 31, 1965
- Mr. Guðmundur Í. Guðmundsson; November 20, 1959 - November 14, 1963
- Mr. Guðmundur Í. Guðmundsson; December 23, 1958 - November 20, 1959
- Mr. Guðmundur Í. Guðmundsson; July 24, 1956 - December 23, 1958
- Mr. Kristinn Guðmundsson; September 11, 1953 - July 24, 1956
- Mr. Bjarni Benediktsson; March 14, 1950 - September 11, 1953
- Mr. Bjarni Benediktsson; December 6, 1949 - March 14, 1950
- Mr. Bjarni Benediktsson; February 4, 1947 - December 6, 1949
- Mr. Ólafur Thors; October 21, 1944 - February 4, 1947
- Mr. Vilhjálmur Þór; December 16, 1942 - October 21, 1944
- Mr. Ólafur Thors; May 16, 1942 - December 16, 1942
- Mr. Stefán Jóh. Stefánsson; November 18, 1941 - January 17, 1942

#### **Ministers who handled foreign affairs in former governments:**

- Mr. Stefán Jóh. Stefánsson; April 17, 1939 - November 18, 1941
- Mr. Hermann Jónasson; April 2, 1938 - April 17, 1939
- Mr. Haraldur Guðmundsson; July 29, 1934 - April 2, 1938
- Mr. Ásgeir Ásgeirsson; June 3, 1932 - July 29, 1934
- Mr. Tryggvi Þórhallsson; August 28, 1927 - June 3, 1932
- Mr. Jón Þorláksson; June 26, 1926 - August 28, 1927
- Mr. Jón Magnússon; March 22, 1924 - June 26, 1926
- Mr. Sigurður Eggerz; March 7, 1922 - March 22, 1924

- Mr. Jón Magnússon; December 1, 1918 - March 7, 1922



## Össur Skarphéðinsson

Date of Birth: June 19th, 1953

Telephone: +354 5630 500

E-mail: [ossur@althingi.is](mailto:ossur@althingi.is)

Party: The Social Democratic Alliance

- Chairman of the Social Democratic Alliance 2000-2005.

### Parliamentary Career

- Member of Althingi for the Reykjavik Constituency 1991-2003, the Reykjavik North Constituency 2003-2009, the Reykjavik South Constituency 2009-2013 and the Reykjavik North Constituency since 2013.

### Party Group

- Chairman of the parliamentary group of the Social Democratic Alliance 2006-2007.
- Chairman of the parliamentary group of the Social Democratic Party 1991-1993.
- Vice-Chairman of the parliamentary group of the Social Democratic Party 1995-1996.

### Present committees

- Member of the Foreign Affairs Committee since 2013, 2005-2007 and 1995-1999 (Vice-Chairman 1998-1999).
- Member of the Icelandic Delegation to the NATO Parliamentary Assembly since 2013 and 2005-2007 (Chairman 2005-2007).

### Earlier committees

- Member of the Credentials Committee 2013.
- Member of the Economy and Trade Committee 2001-2005.
- Member of the Budget Committee 1999-2001.
- Member of the Environment Committee 1999-2000.
- Member of the Health and Social Security Committee 1995-1999 (Chairman 1995-1999).
- Member of the Agriculture Committee 1992-1993 (Vice-Chairman 1992-1993).
- Member of the Industry Committee 1991-1993 (Chairman 1991-1993).
- Member of the Fisheries Committee 1991-1993 (Vice-Chairman 1991-1993).
- Member of the General Affairs Committee on 1991-1992 (Vice-Chairman 1991-1992).

- Member of the Icelandic Delegation to the Parliamentary Assembly of the Council of Europe 2003-2005.
- Member of the Icelandic Delegation to the WEU Assembly 1995-1999 (Vice-Chairman 1995-1999).
- Member of the Icelandic Delegation to the EFTA and EEA Parliamentary Committees 1991-1993 and 1999-2004.

### Ministerial Career

- Minister for Foreign Affairs 2009-2013.
- Minister of Industry 2007-2009.
- Minister for Nordic Co-operation 2007-2008.
- Minister for the Environment 1993-1995.

---

©Secretariat of Althingi  
[Contact us](#)



[illegible] $\mathbf{V}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**PROSECUTION MOTION  
FOR JUDICIAL NOTICE**

**Enclosure 13**

24 June 2013

## Acronyms for PE 30

Time	Page #	Context	Translation
10:17:45am	2	OSINT	Open source intelligence
10:21:34am	3	BI MTF	Bisexual male to female
10:27:06am	3	BTW	By the way
10:28:06am	3	DADT	Don't ask don't tell
10:42:55am	4	OGA	Other government agency
10:45:18am	4	s/If/If I	Substitute "If" for "If I"
11:01:44am	5	K	Okay
11:01:47am	5	TTYL	Talk to you later
12:26:09pm	8	YT?	You, too?
12:53:41pm	9	s/Hilary/Hillary	Substitute "Hilary" for "Hillary"
12:56:43pm	9	<3	Love
1:48:50pm	10	Yanno?	You know?
1:56:43pm	11	PGP	Pretty good privacy
2:02:34pm	11	IDK	I don't know
2:18:56pm	12	AFAIK	As far as I know
2:21:22pm	12	BRB	Be right back
8:06:55am	18	TWYS	Talk with you soon
12:13:25pm	21	Cx	Connection
2:23:51pm	24	cos	Because
2:26:18pm	24	s/only/only see/	Substitute "only" for "only see".
2:52:31pm	26	SOL	Shit out of luck
3:02:19pm	26	s/you/so	Substitute "you" for "so".
3:03:38pm	26	iono	I do not know
3:31:48pm	27	s/a/the	Substitute "a" for "the"
3:40:33pm	28	BRB	Be right back
7:34:52am	31	Str8	Straight, in reference to sexual preference
2:32:58am	35	kk	Okay
2:33:03am	35	FWIW	For what it is worth
3:17:36am	35	NVM	Never mind
3:18:16am	35	t/y	Thank you
3:31:33am	36	rly	Really
1:38:43pm	36	g'day	Good day
1:40:18pm	36	WTF	What the fuck

## Acronyms for PE 30

2:04:05pm	39	pfift	Equivalent to a dismissal of a comment or a lack of interest
2:30:09pm	40	n/p	No problem
2:53:28pm	41	Infowise	Information wise
3:32:29pm	43	FFS	Facial feminizing surgery
3:57:29pm	45	cred	credentials
4:39:38PM	47	WL	Wikileaks
6:11:50pm	49	LTR	Long term relationship

# Acronyms for PE 123

Date	Time	Page #	Context	Translation
5 March 2010	21:12:38	1	&gt;nod&lt;	Acknowledgment to a previous statement; equivalent to nodding your head
5 March 2010	21:17:31	1	&gt;yawn&lt;	yawn
5 March 2010	21:20:54	1	=)	Smile
5 March 2010	22:53:22	1	Ping	Written attempt to determine connectivity between users
6 March 2010	00:39:19	1	=P	sticking your tongue out
6 March 2010	07:08:11	2	XD	Laughing
7 March 2010	07:08:29	3	8RB	Be right back
7 March 2010	07:19:51	3	8TW	by the way
7 March 2010	07:23:52	3	BBK	be back ok?
7 March 2010	07:23:59	3	TTYL	Talk to you later
8 March 2010	05:48:43	4	Heya!	Hello
8 March 2010	06:05:29	4	s/mothers/months	Substitute mothers for months, to correct a previous line that mistakenly included mothers
8 March 2010	06:28:29	5	OFAFBU	One flight away from being ugly
8 March 2010	06:35:30	6	Cya	See you later
8 March 2010	12:21:39	6	ETA	Estimated time of arrival
8 March 2010	12:22:33	6	Mb	Megabytes
10 March 2010	03:45:11	6	SFTP	Secure file transfer program
10 March 2010	06:00:40	7	WTF	What the fuck
10 March 2010	21:00:30	9	Mhmm	non-verbal affirmative
16 March 2010	22:34:24	10	^ ^	Pleasant smile
17 March 2010	22:45:44	10	;)	Winking
17 March 2010	22:48:55	11	K	Okay

## UNITED STATES

 $\mathbf{v}_i$ 

**MANNING, Bradley E., PFC**

U.S. Army,

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE RESPONSE TO  
GOVERNMENT REQUEST FOR  
JUDICIAL NOTICE DATED  
24 JUNE 2013**

DATED: 25 JUNE 2013

1. PFC Bradley E. Manning, by and through counsel, moves this court to deny the Government request for judicial notice in part.

2. As the moving party, the Government has the burden of persuasion. RCM 905(c)(2). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting Government property, and two specifications of knowingly exceeding authorized access to a Government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred to a general court-martial on 3 February 2012.

5. The Defense does not request any witnesses be produced for this motion.

## LEGAL AUTHORITY AND ARGUMENT

6. In the interest of judicial economy, MRE 201 relieves a proponent from formally proving certain facts that reasonable persons would not dispute. There are two categories of adjudicative facts that may be noticed under the rule. First, the military judge may take judicial notice of adjudicative facts that are “generally known universally, locally, or in the area pertinent to the event.” MRE 201(b)(1). Under this category of adjudicative facts, it is not the military judge’s knowledge or experience that is controlling. Instead, the test is whether the fact is generally known by those that would have a reason to know the adjudicative fact. *U.S. v. Brown*, 33 M.J. 706, 709 (N.M.C.A. 1992). The second category of adjudicative facts is those “capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” MRE 201(b)(2). This category of adjudicative facts includes government records, business records, information in almanacs, scientific facts, and well documented reports. *Id.* See also *U.S. v. Spann*, 24 M.J. 508 (A.F.C.M.R. 1987). The key requirement for judicial notice under this category is that the source relied upon must be reliable. Salzburg, Lee D. Schinasi & David A. Schlueter, *Military Rules of Evidence*, §201.02[3] at p. 2-7 (7th Ed., Matthew Bender & Co. 2011)

7. Under MRE 201(d), a military judge should take judicial notice if the proponent presents the necessary supporting information. In making the determination whether a fact is capable of being judicially noticed, the military judge is not bound by the rules of evidence. *Id.* Additionally, the information relied upon by the party requesting judicial notice need not be otherwise admissible. *Id.* The determination of whether a fact is capable of being judicially noticed is a preliminary question for the military judge. See MRE 104(a).

8. Judicial notice is of adjudicative facts. Judicial notice is not appropriate for inferences a party hopes the fact finder will draw from the fact(s) judicially noticed. Legal arguments and conclusions are not adjudicative facts subject to judicial notice. *U.S. v. Anderson*, 22 M. J. 885 (A.F.C.M.R. 1985) (appropriate to take judicial notice of the existence of a treatment program at a confinement facility but not appropriate to take judicial notice of the quality of the program.). See Appellate Exhibit 356.

9. The Defense objects to this Court taking judicial notice of the following requests by the Government:

a. **Wikileaks released a video titled “Collateral Murder” on 5 April.** The Defense objects based on relevance. Whether or not Wikileaks released the aforementioned video on 5 April is not relevant to Specification 2 of Charge II. In order for the Government’s theory of relevance to be accepted, the Court would have to assume that Wikileaks only releases information that is “closely held” within the meaning of 18 U.S.C. § 793. The only issue that is relevant is whether the charged video was closely held or not at the time of PFC Manning’s disclosure. Its subsequent status and the release date by Wikileaks has no bearing on any fact at issue.

b. **Wikileaks released more than 390,000 records from the CIDNE Iraq database on 22 October 2010.** The Defense objects on the basis of relevance. For the reasons

stated above, the release of the records from the charged database is not relevant to determine whether or not the records were closely held. Additionally, the release of these records from the charged database does not make it more probable than not that PFC Manning stole, purloined, or converted the CIDNE Iraq database. The fact that Wikileaks, or any other news organization, published excerpts from the database on a particular date is irrelevant. Thus, any action by Wikileaks outside the period of charged misconduct is not relevant to the charged offense.

c. **Wikileaks released more than 75,000 records from the CIDNE Afghanistan database on 25 July 2010.** The Defense objects on the basis of relevance. For the reasons stated above in (a) and (b), the Defense opposes the Government's request for judicial notice.

d. **Wikileaks released more than 700 detainee assessment briefs produced by JTF-GTMO on 25 April 2011.** The Defense objects on the basis of relevance. For the reasons stated above in (a) and (b), the Defense opposes the Government's request for judicial notice.

e. **Wikileaks release of the ACIC document on 15 March 2010.** The Defense objects on the basis of relevance. For the reasons stated above in (a) the Defense opposes the Government's request for judicial notice.

f. **Base salary of a Specialist, E-4 from 2003-2010.** The Defense objects based upon relevance. How much an E-4 makes in a given year is not relevant to how much the charged database is valued for the purposes of 18 U.S.C. § 641. Should the Government wish to introduce evidence of this nature, it is free to do so through its witnesses subject to objection on relevance and the opportunity for the Defense to cross-examine the witness.

g. **Base salary of GS-12, from 2003-2010.** The Defense objects based upon relevance for the reasons stated above in (f).

h. **Existence of AR 25-1, dated 13 NOV 2007 and the definition of "Information System" from AR 25-2.** The Defense objects based upon relevance. PFC Manning is not charged under AR 25-1. While PFC Manning is charged under 25-2, PFC Manning is not charged with a Specification under 25-2 that requires proof of value. The definitions and statements provided by this unrelated regulation do not establish, or help establish, that the charged databases in this case had value. The Government is free to elicit witness testimony that the allegedly stolen, purloined, or converted databases had value. If the Government elects to do so, the Defense will then have the opportunity to object on relevance, personal knowledge, and hearsay grounds. The Defense will also have the opportunity to cross examine the witness. The Government, however, should not be permitted to rely upon an unrelated regulation that has nothing to do with the charged databases to establish value.

i. **Existence of DoD 5400.11-R, dated 14 May 2007.** The Defense objects based upon relevance for the reasons stated above in (h).

j. **Thanksgiving 2009 was on November 26.** The Defense does not object to the fact that Thanksgiving Day occurred on 26 November in 2009.

k. **The term, ".is," is the top-level internet domain of Iceland.** The Defense objects based on relevance. The information is not relevant to prove that PFC Manning acted wantonly as charged in Specification 1 of Charge II. The Court has received testimony from numerous witnesses who testified that PFC Manning was permitted to search for whatever he wanted on the SIPRNET during his work day or free time. As such, any specific search allegedly done by PFC Manning does not make it more likely than not that PFC Manning acted "wantonly" and thus, is not relevant.

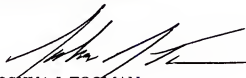
l. **Positions of various Icelandic politicians.** The Defense objects based on relevance for the reasons stated above in (k).

m. **Internet chat lingo and their meanings.** The Defense does not believe that this "lingo" is proper for judicial notice. The Court can use its common sense when reading the chats, but several of the meanings are open to interpretation and thus do not fall within the type of information that can be the subject of judicial notice. The Government is free to provide its interpretation of the various terms in the chat logs through its witnesses. If the Government elects to do so, the Defense will then have the opportunity to object on relevance, personal knowledge, and hearsay grounds. The Defense will also have the opportunity to cross examine the witness.

#### CONCLUSION

10. Based on the above, the Defense requests that the Court deny, in part, the Government's request for judicial notice.

Respectfully Submitted



JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel





REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
U.S. ARMY MILITARY DISTRICT OF WASHINGTON  
103 THIRD AVENUE  
FORT LESLEY J. MCNAIR, DC 20318-5013

ANCG

14 JUN, 2013

MEMORANDUM FOR CPT Steven Lim, G2, First Army Division East, Fort Meade, MD  
20755

SUBJECT: Grant of Testimonial Immunity

1. As an officer empowered to convene general courts-martial and pursuant to Rule for Courts-Martial (R.C.M.) 704, I hereby make the following findings:

a. You possess information relevant to the pending court martial - United States v. PFC Bradley Manning.


b. Based on your privilege against self-incrimination, you may refuse to fully convey the information you possess regarding this case.

c. Your testimony before any court-martial that may be convened to try PFC Manning, and your cooperation with law enforcement officials and counsel investigating allegations that may result in such proceedings, is necessary to the public interest, including the needs of good order and discipline of this command.

2. Based on the above facts and pursuant to R.C.M. 704, I hereby order you to fully cooperate with and provide truthful and complete information to law enforcement officials and counsel during the investigation of PFC Manning, and to further provide truthful and complete testimony before any administrative board or court-martial convened to process or try PFC Manning.

3. No testimony or other information given by you pursuant to this order or any information directly or indirectly derived from such testimony shall be used against you in a criminal case or under Article 15, UCMJ, except in a prosecution for perjury, giving a false statement, or otherwise failing to comply with this order.

4. The grant of immunity embodied in this order constitutes a grant of testimonial immunity pursuant to R.C.M. 704(a)(2) and becomes effective upon service on CPT Lim by the trial counsel assigned to United States v. PFC Bradley Manning.

  
MICHAEL S. LINNINGTON  
Major General, U.S. Army  
Commanding

APPELLATE EXHIBIT 578  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

UNITED STATES )

v. )

**POST-TRIAL AND APPELLATE  
RIGHTS**

**(General Court-Martial)**

**MANNING, Bradley E., PFC** )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

DATED: 15 July 2013

---

I, **PFC Bradley E. Manning**, the accused in the above entitled case, certify that my trial defense counsel and my civilian defense counsel have advised me of the following post-trial and appellate rights in the event that I am convicted of a violation of the Uniform Code of Military Justice.

1. In exercising my post-trial rights, or in making any decision to waive them, I am entitled to the advice and assistance of military counsel provided free of charge or civilian counsel provided at no expense to the government.
2. After the record of trial is prepared, the convening authority will act on my case. The convening authority can approve the sentence adjudged (as limited by any pretrial agreement), or he can approve a lesser sentence, or disapprove the sentence entirely. The convening authority cannot increase the sentence. He can also disapprove some or all of the findings of guilty. The convening authority is not required to review the case for legal errors, but may take action to correct them.
3. Under Rules for Court-Martial 1105 and 1106, I have the right to submit any matters to the convening authority that I wish him to consider in deciding what action to take in my case. These matters include, but are not limited to, a personal statement, personal letters and documents, letters and documents from any other person, requests for deferment and waiver of forfeitures, and any other matter I desire the convening authority to consider before taking action in my case.
  - a. Before the convening authority takes action, the staff judge advocate will submit a recommendation to the convening authority. This recommendation will be sent to me and/or my defense counsel before the convening authority takes action.
  - b. If I have matters that I wish the convening authority to consider, or matters in response to the staff judge advocate's recommendation, such matters must be submitted within 10 days after I receive a copy of the record of trial or the recommendation of the staff judge advocate, whichever occurs later. If I authorize substitute service in accordance with paragraph 12 of this form, the 10 day period begins to run after my counsel receives the record of trial or the staff judge advocate's recommendation, whichever occurs later.
  - c. Upon my request, the convening authority may extend this period, for good cause, for not more than 20 days.

d. I understand that I must work with my defense counsel to assist him/her in collecting and preparing those matters I want to be submitted to the convening authority, and in that regard I must remain in contact with my defense counsel even after my case has been tried.

§ 1 e. (Strike through inapplicable portions). I (authorize) (~~do not authorize~~) my defense counsel to submit matters pursuant to RCM 1105 and 1106 on my behalf in the event that he is unable to contact me after making reasonable efforts to find me in accordance with TDS policy.

4. If the convening authority approves an adjudged punitive discharge (dismissal for officers; bad-conduct or dishonorable discharge for enlisted soldiers) or confinement for one year or longer, my case will be automatically reviewed by the Army Court of Criminal Appeals (ACCA). I am entitled to be represented by counsel before such court. If I so request, military counsel will be appointed to represent me at no cost to me. If I so choose, I may also be represented by civilian counsel at no expense to the United States.

5. After the ACCA completes its review, I may petition the United States Court of Appeals for the Armed Forces (CAAF) to review my case. If that Court grants my petition, I may request review by the Supreme Court of the United States. I have the same rights to counsel before those courts as I have before the ACCA. If I am pending an approved dishonorable or bad-conduct discharge it may only be ordered executed after completion of the appellate process in accordance with Rule for Court-Martial 1209, unless I waive appellate review.

6. If the convening authority approves no punitive discharge and approves confinement for less than a year, my case will be examined in the Office of The Judge Advocate General for any legal errors and to determine if the sentence is appropriate. The Judge Advocate General (TJAG) may take corrective action as appropriate. This mandatory review under Article 69(a), UCMJ, will constitute the final review of my case unless TJAG directs review by the ACCA.

7. I may waive or withdraw review by the appellate courts after action has been taken by the Convening Authority. I cannot waive or withdraw appellate review before action. I understand that if I waive or withdraw review:

a. My decision is final and I cannot change my mind.

b. My case will then be reviewed by a military lawyer for legal error. It will also be sent to the general court-martial convening authority for final action.

c. Within two (2) years after the sentence is approved, I may request The Judge Advocate General (TJAG) to take corrective action on the basis of newly discovered evidence, fraud on the court-martial, lack of jurisdiction over me or the offense, error prejudicial to my substantial rights, or the appropriateness of the sentence.

8. I understand that any period of confinement included in my sentence begins to run from the date the court-martial adjudges my sentence. I may request that the convening authority defer commencement of confinement. The decision to defer confinement is within the sole discretion of the convening authority.

9. Adjudged forfeitures and reduction in rank.

a. Any forfeitures adjudged in my case are effective 14 days after the sentence is adjudged or when the convening authority takes action, whichever occurs first, unless adjudged forfeitures are deferred. If forfeitures are adjudged at the court-martial, I understand that I may petition the convening authority to defer them until action and to disapprove, mitigate, or suspend them at action.

b. Adjudged reduction (enlisted personnel only). Any reduction in rank adjudged in my case is effective 14 days after the sentence is adjudged or when the convening authority takes action, whichever occurs first, unless the reduction is deferred. If a reduction is adjudged at the court-martial, I understand that I may petition the convening authority to defer a reduction in rank until action and to disapprove or suspend it at action.

10. Automatic forfeitures. I understand that by operation of Article 58b of the Uniform Code of Military Justice, any sentence that includes confinement for more than 6 months, or confinement for 6 months or less and a punitive discharge, will result in automatic forfeitures during any period of confinement even if no forfeitures are adjudged. In the case of a General Court-Martial, automatic forfeitures are for all pay and allowances. In a Special Court-Martial, the automatic forfeitures are for two-thirds of pay. Automatic forfeitures go into effect 14 days after my sentence is adjudged or when the convening authority takes action, whichever occurs first.

RCM a. I understand I may petition the convening authority to defer adjudged or automatic forfeitures, if any, until the time of final action, but such relief is solely within the discretion of the convening authority, who may rescind deferment at any time.

RCM b. I understand that if I reach my ETS date while I am in confinement all my pay and allowances will stop on my ETS date, even if a request for deferment or waiver of automatic forfeitures is granted.

RCM c. I further understand that if I reach my ETS date while I am in confinement all my pay and allowances will stop on my ETS date, even if a request for deferment or disapproval of adjudged forfeitures is granted.

RCM d. *(Applicable if accused has a pretrial agreement)* I further understand that if I reach my ETS date while I am in confinement all my pay and allowances will stop on my ETS date, regardless of what is in my pretrial agreement.

RCM e. I understand that if adjudged forfeitures are not deferred or disapproved, I will not receive pay even if automatic forfeitures are waived.

11. I have read and had my post-trial rights explained to me by counsel and I acknowledge these rights and make the elections set forth below.

RCM a. I understand my post-trial and appellate review rights.

RCM b. I understand that a copy of the authenticated record of trial will be served on me, or if I so request, will be forwarded to my defense counsel pursuant to RCM 1104(b).

Select only one of the following three numbered options. Option (4) is the recommended best option in most cases. If you use option (2), be sure to select the appropriate language and eliminate the excess language.

\_\_\_\_ (1) I want the record of trial sent to only me; or

\_\_\_\_ (2) **(Indicate counsel.)** I authorize substitute service of the ROT if the SJAR and ROT are served (two weeks) before (I complete my term of confinement) (my minimum release date)(specify a date) (the 120th day after the sentence in my case was announced). If the SJAR and ROT are served (two weeks) before (I complete my term of confinement) (my minimum release date) (specify a date) (the 120th day after the sentence in my case was announced), the record of trial may be served on my defense counsel, \_\_\_\_\_. If the SJAR and ROT are not served (two weeks) before (I complete my term of confinement) (my minimum release date)(specify a date) (the 120th day after the sentence in my case was announced), the record of trial shall be served on me; or

\_\_\_\_ (3) **(Indicate counsel.)** I want the record of trial forwarded to my defense counsel, \_\_\_\_\_; or

RCM (4) **(Indicate counsel.)** I want the record of trial sent to me AND I request that my defense counsel MR. DAVID E. COOMBS be provided a copy at the same time I receive my copy in order to expedite preparation of post-trial matters.

RCM c. I further understand that individual copies of the staff judge advocate's post trial recommendation will be served on me and my defense counsel pursuant to RCM 1106(f).

RCM d. **(Indicate counsel.)** My defense counsel MR. DAVID E. COOMBS, will submit R.C.M. 1105 and 1106 matters in my case if I desire. I further understand that I must stay in contact with this counsel to assist him in collecting and preparing the matters for submission.

12. **(Strike through inapplicable portions.)** ~~My counsel (has) (has not) advised of me of the criteria which require registration as a sex offender.~~

13. **(Strike through inapplicable portions.)** ~~My counsel (has) (has not) advised me of the possible adverse consequences a conviction may have on my immigration status.~~

14. I understand that if my case is to be heard by the Army Court of Criminal Appeals, I have the right to be represented free of charge by Appellate Defense Counsel appointed by The Judge Advocate General (TJAG) of the Army. I may also waive this right after the Convening Authority takes action. I understand that I may contact my Appellate Defense Counsel by writing to Defense Appellate Division, U.S. Army Legal Services Agency (JALS-DA). Phone: (703) 693-0649. DSN: 223-0649.

RCM I have been informed that I have the right to retain civilian counsel at my own expense to represent me in my appellate decisions. If I have already retained civilian counsel, his/her name and address is written below:


---

RCM If I later retain civilian counsel, I must provide the attorney's name and address to: Clerk of Court, The U.S. Army Court of Criminal Appeals, 9275 Gunston Road, Fort Belvoir, VA 22060. Phone: (703) 693-1309. DSN: 223-1309. FAX: (703) 806-0124. DSN 223-0124.

15. Pending action on my case, I can be contacted or a message may be left for me at the following address:

NAME: MS. DEBRA M. VAN ALSTINE (C/O)  
STREET: 1492 SELWORTHY ROAD  
CITY/ STATE / ZIP CODE: POTOMAC, MARYLAND 20854  
AREA CODE / TELEPHONE NUMBER: (301) 738 7816  
EMAIL ADDRESS: \_\_\_\_\_  
CIVILIAN / PERMANENT EMAIL ADDRESS: \_\_\_\_\_  
PERSONAL CONTACT: \_\_\_\_\_

Date: 15 JULY 2013

  
BRADLEY EDWARD MANNING  
PFC, US Army  
Accused

I certify that I have advised PFC Bradley Manning regarding his post-trial and appellate rights as set forth above, that he has received a copy of this document, and that he has personally made all the elections herein.

Date: 15 JULY 2013

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel



REPLY TO  
ATTENTION OF:

DEPARTMENT OF THE ARMY  
U.S. ARMY MILITARY DISTRICT OF WASHINGTON  
102 3RD AVENUE, BLDG 39, SUITE 2  
FORT LESLEY J. MCNAIR, DC 20319-5031

ANCG

June 24, 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Assumption of Command By Authority of Paragraph 2-6, AR 600-20

The undersigned assumes command of United States Army Military District of Washington (WOGVAA), Fort Lesley J. McNair, DC 20319, effective 0001, 24 June 2013

A handwritten signature in black ink, appearing to read "Jeffrey S. Buchanan", is written over the typed name.

JEFFREY S. BUCHANAN  
MG, US Army  
Commanding

DISTRIBUTION:  
A

**UNITED STATES OF AMERICA**

**v.**

**Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211**

**Witness List Order  
for the Defense  
Witnesses**

**25 June 2013**

The Defense hereby submits the following order for the first ten witnesses the Defense intends to call in the above-captioned court-martial:

1. CW2 Joshua Ehresman
2. CPT Barclay Keay
3. SGT David Sadtler
4. Ms. Lauren McNamara
5. Col(r) Morris Davis

6. Mr. Cassius Hall
7. Mr. Charles Ganiel
8. Stipulation – Defense Exhibit B
9. Professor Yochai Benkler
10. Mr. Trent Struttman



**DAVID EDWARD COOMBS**  
Civilian Defense Counsel



UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**RULING: Motions by Parties  
for Judicial Notice of  
Adjudicative Facts**

27 June 2013

**Defense Requested Judicial Notice** - On 15 June 2013, the Defense filed 3 motions for judicial notice (AE 569 – 571) requesting the Court to take judicial notice of the following adjudicative facts:

1. The 13 October 2010 classification assessment conducted by RADM Kevin Donegan, Director of Operations at CENTCOM, regarding the Apache Video (PE 15).
2. The audio transcript for PE 15.
3. On or about 25 November 2009, WikiLeaks published what it claimed to be text and pager messages sent on 11 September 2001. The Defense does not request the Court to take judicial notice of the messages themselves or that the messages are actually from 11 September 2001.
4. On 25 July 2007, Reuters made a FOIA request to DoD for video and audio recordings relating to the deaths of Mr. Namir Noor-Eldeen and Mr. Saeed Chmagh, Reuters journalists. CENTCOM responded to the Reuters request on 24 April 2009.

On 19 June 2013, the Government filed a brief opposing (1), (2), and (4) above (AE 574). After oral argument, the Government revised its position and did not object to (2), (3), and (4) above. The parties stipulate that Enclosure 2 to AE 574 is an accurate transcript of the audio of PE 15. The Government objected to the classification assessment in (1) as hearsay not admissible as a statement of a party opponent under MRE 802(d)(2)(D).

The Court will grant Judicial Notice for (2), (3), and (4). The only remaining issue regarding the Defense motions for judicial notice is whether the Court will take judicial notice of (1).

**Government requests for Judicial Notice** - On 25 June 2013, the Government filed a motion for Judicial Notice (corrected copy) at AE 576 moving the Court to take notice of the following adjudicative facts:

**Adjudicative Facts: WikiLeaks Releases**

- a. WikiLeaks released a video titled "Collateral Murder" on 5 April 2010;

b. WikiLeaks released more than 390,000 records from the Combined Information Data Network Exchange (CIDNE) Iraq database on 22 October 2010;

c. WikiLeaks released more than 75,000 records from the CIDNE Afghanistan database on 25 July 2010;

d. WikiLeaks released more than 700 detainee assessments produced by Joint Task Force Guantanamo (JTF-GTMO) on 25 April 2011;

e. WikiLeaks released a memorandum produced by the Army Counterintelligence Center titled "Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 15 March 2010;

#### **Adjudicative Facts: Salary of Servicemembers and Government Employees**

f. The monthly base salary for Servicemembers at the rank of Specialist, E-4, was \$1,502.70 in 2003, \$1,558.20 in 2004, \$1,612.80 in 2005, \$1,662.90 in 2006, \$1,699.50 in 2007, \$1,758.90 in 2008, \$1,827.60 in 2009, and \$1,889.70 in 2010;

g. The yearly base salary for government employees at the grade of 12 on the General Schedule (GS) scale was \$51,508 in 2003, \$52,899 in 2004, \$54,221 in 2005, \$55,360 in 2006, \$56,301 in 2007, \$57,709 in 2008, \$59,383 in 2009, and \$60,274 in 2010;

#### **Adjudicative Facts: Reference Materials**

h. The existence of Army Regulation (AR) 25-1, dated 13 November 2007, specifically paragraphs 1-1, subparagraphs (a) and (b) of 1-7, and subparagraphs (d), (e), and (f) of 6-1 and the definition found in AR 25-2 of "Information System;"

i. The existence of DoD 5400.11-R: Department of Defense Privacy Program, dated 14 May 2007, specifically Appendix 1 and the definition of "Personal Information;"

#### **Adjudicative Facts: Miscellaneous**

j. Thanksgiving of 2009 occurred on 26 November 2009;

k. The term, ".is," is the top level internet domain of Iceland;

l. Johanna Sigurdardottir was the Prime Minister of Iceland from February 2009 – May 2013, Ossur Skarphedinsson was the Icelandic Minister for Foreign Affairs from February 2009 – May 2013, Albert Jonsson was the Icelandic Ambassador to the United States from 2006-2009, and Birgitta Jonsdottir has been a member of the Icelandic parliament since 2009; and

m. The Internet chat lingo and their meanings in Enclosure 13 are synonymous.

On 25 June 2013, the Defense filed a brief objecting to all of the above except (j) and (m) on the grounds of relevance. The Defense did not object to (j) and objected to (m) as an improper subject for judicial notice. At oral argument, the Defense conceded that (a) – (l) were properly judicially noticed adjudicative facts if relevant. Thus, with the exception of (j), all of the Government's motions for judicial notice remain at issue.

#### **The Law: Judicial Notice**

1. Military Rule of Evidence (MRE) 201 governs judicial notice of adjudicative facts. The judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known universally, locally, or in the area pertinent to the event or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. *U.S. v. Needham*, 23 M.J. 383 (C.M.A. 1987); *U.S. v. Brown*, 33 M.J. 706 (A.C.M.R. 1991).
2. MRE 201(c) requires the military judge to take judicial notice of adjudicative facts if requested by a party and supplied with the necessary information.
3. When the military judge takes judicial notice of adjudicative facts, the fact finder is instructed that they may, but are not required to, accept as conclusive any matter judicially noticed.
4. Judicial notice is of adjudicative facts. Judicial notice is not appropriate for inferences a party hopes the fact finder will draw from the fact(s) judicially noticed. Legal arguments and conclusions are not adjudicative facts subject to judicial notice. *U.S. v. Anderson*, 22 M.J. 885 (A.F.C.M.R. 1985) (appropriate to take judicial notice of the existence of a treatment program at a confinement facility but not appropriate to take judicial notice of the quality of the program.).

#### **The Law: Hearsay**

1. Hearsay is a statement, other than the one made by the declarant while testifying at the trial, offered in evidence to prove the truth of the matter asserted. MRE 801(c). Hearsay is not admissible except as provided by the Military Rules of Evidence or by any Act of Congress applicable in trials by court-martial. MRE 802.
2. Admission by a Party Opponent. MRE 801(d)(2)(D) provides in relevant part that admissions by a Party Opponent are not hearsay if the statement is offered against a party and is a statement by the party's agent or servant concerning a matter within the scope of the agency or employment of the agent or servant made during the existence of the relationship....The contents of the statement shall be considered but are not alone sufficient to establish the declarant's ....agency or employment relationship and the scope thereof under (D). Consistent with the Court's 18 October 2012 Ruling: Defense Motion: Motion for Judicial Notice of Adjudicative facts – Finkel Book and Public statements (AE 356), the Court adopts the three-part test adopted by the Second Circuit in *United States v. Salerno*, 937 F.2d 797, 811 (2<sup>nd</sup> Cir. 1991) to determine if the classification assessment by RADM Donegan qualifies as an admission under MRE 801(d)(2)(D) against the Government and is worthy of judicial notice. The three-part test requires the Court, "[to] be satisfied that the prior [statement] involves an assertion of fact

inconsistent with similar assertions in a subsequent trial. Second, the court must determine that the [statements] were such as to be the equivalent of testimonial statements.... Last, the district court must determine by a preponderance of the evidence that the inference that the proponent of the statements wishes to draw is a fair one and that an innocent explanation for the inconsistency does not exist.” *Salerno*, 937 F.2d at 811 (2d Cir. 1991) (quoting *United States v. McKeon*, 738 F.2d 26, 33 (2d Cir. 1984) (quotations omitted); see also *United States v. DeLoach*, 34 F.3d 1001, 1005 (11th Cir. 1994) (adopting the test from *Salerno*). The fact that a statement is admissible against a party opponent does not bind the party to that statement. The party against whom such a statement is made can rebut the statement and assert a different or contrary position. *U.S. v. Bellamy*, 403 Md. 308, 328, fn. 19.

**The Law: Use of Statements Made by an Accused during the Providence Inquiry in the Merits of the Trial.** An accused’s guilty plea to a lesser included offense may be used to establish elements of the greater offense during the contested portions of the trial. Statements made by the accused during the providence inquiry, whether orally or in writing, are not evidence that is before the trier of fact and may not be considered during the contested portion of the trial. RCM 913(a) Discussion; *U.S. v. Grijalva*, 55 M.J. 223 (C.A.A.F. 2001).

#### **Conclusions of Law:**

#### **Defense Motion for Judicial Notice of Classification Assessment of RADM Donegan.**

1. The Court will not consider any statements made by the accused during the providence inquiry as evidence to support any of the requests for judicial notice.
2. RADM Donegan’s statement meets the *Salerno* test and qualifies as an admission of a party opponent under MRE 801(d)(2)(D). RADM Donegan was acting in his official capacity as Director of Operations, CENTCOM, when he made the classification assessment. The classification assessment states facts inconsistent with the Stipulation of Expected Testimony of CW5 John Larue at PE 117. The inference the Defense wishes to draw is a fair one.
3. The Court will take Judicial Notice of the 13 October 2010 classification assessment by RADM Donegan.

**Government Motion for Judicial Notice.** The facts in (a) – (l) are adjudicative facts capable of accurate and ready determination of by resort to sources whose accuracy cannot reasonably be questioned.

#### **Adjudicative Facts: WikiLeaks Releases**

- a. WikiLeaks released a video titled “Collateral Murder” on 5 April 2010;
- b. WikiLeaks released more than 390,000 records from the Combined Information Data Network Exchange (CIDNE) Iraq database on 22 October 2010;

c. WikiLeaks released more than 75,000 records from the CIDNE Afghanistan database on 25 July 2010;

d. WikiLeaks released more than 700 detainee assessments produced by Joint Task Force Guantanamo (JTF-GTMO) on 25 April 2011;

e. WikiLeaks released a memorandum produced by the Army Counterintelligence Center titled "Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 15 March 2010;

All of the Wikileaks releases are relevant to show the path of information allegedly from the accused through WikiLeaks with opportunity to access it by the enemy for the specification of Charge I (Aiding the Enemy) and for the caused to be published element of specification 1 of Charge II (Wantonly Caused to be Published). In addition (a) – (e) are relevant to facts at issue as to whether the accused stole, purloined, or knowingly converted information and whether the information was closely held by the Government for the following specifications of Charge II: (a) - specification 2; (b) – specifications 4 and 5; (c) – specifications 6 and 7; (d) specifications 8 and 9; and (e) specification 15. The Court will take judicial notice of (a) – (e).

#### **Adjudicative Facts: Salary of Servicemembers and Government Employees**

f. The monthly base salary for Servicemembers at the rank of Specialist, E-4, was \$1,502.70 in 2003, \$1,558.20 in 2004, \$1,612.80 in 2005, \$1,662.90 in 2006, \$1,699.50 in 2007, \$1,758.90 in 2008, \$1,827.60 in 2009, and \$1,889.70 in 2010;

g. The yearly base salary for government employees at the grade of 12 on the General Schedule (GS) scale was \$51,508 in 2003, \$52,899 in 2004, \$54,221 in 2005, \$55,360 in 2006, \$56,301 in 2007, \$57,709 in 2008, \$59,383 in 2009, and \$60,274 in 2010;

The monthly and yearly base salaries of Servicemembers and government employees in the grade of GS 12 are relevant to a fact in issue to prove value of the information in specifications 8 and 16 of Charge II. The Court will take judicial notice of (f) and (g).

#### **Adjudicative Facts: Reference Materials**

h. The existence of Army Regulation (AR) 25-1, dated 13 November 2007, specifically paragraphs 1-1, subparagraphs (a) and (b) of 1-7, and subparagraphs (d), (e), and (f) of 6-1 and the definition found in AR 25-2 of "Information System;"

i. The existence of DoD 5400.11-R: Department of Defense Privacy Program, dated 14 May 2007, specifically Appendix 1 and the definition of "Personal Information;"

The references in AR 25-1, AR 25-2, and DoD 5400-R are relevant to a fact at issue in specification 16 of Charge II – to prove that the information stolen was a thing of value to the United States and are also relevant to a fact at issue in specification 4 of Charge III - to prove

that the accused used an information system for a manner other than its intended use. The Court will take judicial notice of (h) and (i).

**Adjudicative Facts: Miscellaneous**

j. Thanksgiving of 2009 occurred on 26 November 2009;

k. The term, “.is,” is the top level internet domain of Iceland;

l. Johanna Sigurdardottir was the Prime Minister of Iceland from February 2009 – May 2013, Ossur Skarphedinsson was the Icelandic Minister for Foreign Affairs from February 2009 – May 2013, Albert Jonsson was the Icelandic Ambassador to the United States from 2006-2009, and Birgitta Jonsdottir has been a member of the Icelandic parliament since 2009; and

m. The Internet chat lingo and their meanings in Enclosure 13 are synonymous.

The Defense does not object to the Court taking judicial notice of (j). The terms and names in (k) and (l) were used by the accused in searches on Intelink and chats with Press Association/Julian Assange (PEs 81; 123; and 127). The facts at (k) and (l) are relevant to explain to the fact-finder the terms used in the searches and chats by the accused and are also relevant to whether the accused acted wantonly for specification 1 of Charge II (Wantonly Caused to be Published). The Government has provided no references for (m) other than a chart of chat terms and translations prepared by an unknown person or entity. The facts at (m) are not adjudicative facts capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. The Court will take judicial notice of (j), (k), and (l). The Court will not take judicial notice of (m).

**Ruling:** The Defense motions for judicial notice are **Granted**. Government motion for judicial notice is **Granted in Part**. The Court will take judicial notice of (a) – (l). The Court will not take judicial notice of (m) (meanings of internet chat lingo).

So **Ordered** this 27<sup>th</sup> day of June 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Witness List Order  
for the Defense  
Witnesses**

27 June 2013

The Defense hereby submits the following order for the first ten witnesses the Defense intends to call in the above-captioned court-martial:

- |                        |                                    |
|------------------------|------------------------------------|
| 1. CW2 Joshua Ehresman | 6. Col(r) Morris Davis             |
| 2. CPT Barclay Keay    | 7. Mr. Cassius Hall                |
| 3. SGT David Sadtler   | 8. Mr. Charles Ganiel              |
| 4. CPT Steven Lim      | 9. Stipulation – Defense Exhibit B |
| 5. Ms. Lauren McNamara | 10. Professor Yochai Benkler       |

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

)  
)  
) **RULING: GOVERNMENT**  
) **MOTION TO ADMIT**  
) **PROSECUTION EXHIBITS 31, 32,**  
) **AND 109 FOR IDENTIFICATION**

) **DATED: 28 June 2013**  
)

On 10 June 2013, after hearing testimony from Special Agent (SA) Mander, the Court ordered the parties to file briefs on the admissibility of Prosecution Exhibits (PE) 31, 32, and 109 for Identification (ID). On 15 June 2013, the parties filed briefs (Government at AE 567; Defense at AE 568). On 18 June 2013, the Court heard oral argument from counsel. On 27 June 2013, the Government recalled SA Mander and offered PE 31A and B and PE 32A and B for ID into evidence. The Court has considered the filings by the parties, evidence presented, the testimony of Special Agent (SA) Mander, and oral argument of counsel. The Court finds and rules as follows:

On 10 June 2013, the Government offered Prosecution Exhibits (PE) 31, 32, and 109 for ID into evidence through the testimony of SA Mander. On 27 June 2013, the Government offered PEs 31A and B and PEs 32A and B into evidence via additional testimony from SA Mander. The Government offers to authenticate PEs 31, 31A, 31B, 32, 32A, and 32B for ID in accordance with (IAW) MRE 901(b)(1) (Testimony of a Witness with knowledge – SA Mander) and MRE 901(b)(4) (Distinctive Characteristics and the Like: the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances). The Government offers to authenticate PE 109 for ID as a self-authenticating business record IAW MRE 803(6) and MRE 902(11) and IAW MRE 901(b)(1) (Testimony of a Witness With Knowledge) through the testimony of SA Mander and the attestation by Mr. Christopher Butler, Office Manager of archive.org (AE 567, enclosure 1).

**Findings of Fact:**

**PEs 31, 31A, 31B, 32, 32A, and 32B for ID.**

1. PE 31 and 32 for ID are screen captures from Google Cache, a website that archives past versions of other websites. In this case, PE 31 and 32 for ID are Google Cache archives of WikiLeaks' [twitter.com](https://twitter.com) postings. SA Mander is unfamiliar with the process of how google cache archives web postings.
2. WikiLeaks has an account on the twitter website. Twitter accounts post messages in chronological order with the most recent on top. All published messages remain on the site indefinitely. On or about August 2012, SA Mander accessed the WikiLeaks account on twitter through a google search. The WikiLeaks account or "feed" had thousands of messages, making searches for particular tweets onerous directly through the WikiLeaks feed. SA Mander then looked for specific WikiLeaks tweets by using search terms on google. The search terms caused google to pull up the twitter website with the tweets in PE 31A and PE 32A for ID. PE 31A and PE 32A for ID are screen captures taken by SA Mander on or about August 2012 while he was reviewing the WikiLeaks tweets on the twitter



website. SA Mander typed the uniform research locator (URL) address of each tweet in a text box in the screen capture. The URL for PE 31A for ID is <http://www.twitter.com/#!/wikileaks/status/13570878440>. The URL for PE 32A for ID is <http://www.twitter.com/#!/wikileaks/status/7530875613>. SA Mander personally viewed the WikiLeaks twitter account and found that the tweets on the account have the same web address except for a serial number unique to each tweet. SA Mander visited the twitter page for WikiLeaks on or about 3 June 2013 and, again, on 27 June 2013. On 27 June 2013, SA Mander typed in the URL of PE 32A in a google search and retrieved the twitter website with the tweet in PE 32B. From the twitter website, SA Mander then typed in the URL for PE 31A and retrieved the tweet in PE 31B. SA Mander took screen shots of both tweets. PE 31B and PE 32B have the same URL as PE 31A and 32A except that PE 31B and PE 32B begin the URL with "https" rather than "http" and they do not have the "#!/". Nevertheless, a search using the URL for PEs 31A and 32A for ID in google retrieves PEs 31B and 32B for ID. Also on 27 June 2013, SA Mander went directly to the WikiLeaks feed on twitter to try to find the tweets in PE 31 and 32 for ID. The feed would not let him have access to messages prior to March, 2013. SA Mander has never viewed the tweets in PE 31 and 32 for ID directly from the WikiLeaks twitter feed.

3. PEs 31, 31A, 31B, 32, 32A, and 32B for ID have the following distinctive characteristics attributable to WikiLeaks: the tweets feature the WikiLeaks logo; they feature WikiLeaks name as the account name "WikiLeaks" used on Twitter; the serial numbers the URL are the same for PEs 31, 31A, and 31B for ID; the serial numbers for the URL of PEs 32, 32A, and 32B are the same; and the content of the tweets in the PE 31 for ID series of exhibits and the PE 32 for ID series of exhibits relates to the information allegedly compromised by PFC Manning.

4. The date and time of the tweets in PEs 31, 31A, and 31B for ID are the same and are actually on the tweets themselves and not generated from Google.cache or any other internet archive process. PE 31, 31A, and 31B are screen images of the same tweet with the WikiLeaks label, logo, text, time/date, and URL serial number. The same is true for the date and time of the tweets in PEs 32, 32A, and 32B for ID.

#### **PE 109 for ID**

1. PE 109 for ID is a screen capture from [archive.org](http://archive.org), another website that archives past versions of websites from across the internet. More specifically, PE 109 for ID is a webpage from [archive.org](http://archive.org) purporting to show a [WikiLeaks.com](http://wikileaks.com) webpage available on the internet on 5 November 2009 at 06:13:30.

2. SA Mander has not viewed the original [WikiLeaks.com](http://wikileaks.com) webpage that the [archive.org](http://archive.org) webpage purports to have archived as PE 109 for ID. He also has no personal knowledge of the methods or standards employed by [archive.org](http://archive.org) in creating and maintaining their web pages or with methods or standards used to capture web pages by third party donors to [archive.org](http://archive.org).

3. On 15 June 2013, the parties submitted briefs on the admissibility of PE 31, 32, and 109 for ID. As additional evidence to authenticate PE 109 for ID IAW MRE 902(11) and MRE 901(b)(2), the Government submitted an Attestation Certificate from Mr. Christopher Butler, Office Manager of [archive.org](http://archive.org) dated 12 June 2013 (AE 567, Enclosure 1). The attestation reads:

I swear or affirm that each of the following is true regarding the attached records to the best of my knowledge and belief:

1. I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;

2. to the best that the electronic systems involved can accurately record and reflect, such files were captured at or near the time of the date reflected in the URL assigned to each file by virtue of an automated transfer of electronic data.

3. such records were captured by Internet Archive or received from third party donors in the course of regularly conducted business activity by the Internet Archive;

4. The records are true and accurate copies of the original documents in Internet Archive's Wayback Machine service at [web.archive.org](http://web.archive.org).

The Court notes the attached record to this attestation is entitled "Draft: The Most Wanted Leaks of 2009-sort" with the same content and URL as PE 109 for ID.

4. The Defense also submitted an attestation from Mr. Butler dated 13 June 2013 (enclosure 10 of the Defense brief - AE 568). The attestation reads as follows:

1. I am the Office Manager at the Internet Archive, located in San Francisco, California. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to surf more than 240 billion pages stored on the Internet Archive's web archive. Visitors to the Wayback machine can search archives by URL (i.e. a website address). If archived records for a URL are available, the visitor will be presented with a list of available dates. The visitor may select one of those dates and then begin surfing on an archived version of the Web. The links on the archived files, when saved by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the page upon which the link appeared and was clicked.

4. The archived data made viewable and browseable by the Wayback Machine is compiled using software programs known as crawlers, which surf the Web and automatically store copies of web files, preserving these files as they exist at the point of time of capture.

5. The Internet Archive assigns a URL on its site to the archived files in the format [http://web.archive.org/web/\[Year in yyyy\]\[day in dd\]\[Time code in hh:mm:ss\]/\[Archived URL\]](http://web.archive.org/web/[Year in yyyy][day in dd][Time code in hh:mm:ss]/[Archived URL]). Thus, the Internet Archive URL <http://web.archive.org/web/19970126045828/http://www.archive.org/> would be the URL for the record of the Internet Archive home page HTML file (<http://www.archive.org/>) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). A web browser may be set such that a printout from it will display the URL of a web page in the printout's footer. The date assigned by the Internet Archive applies to the HTML file but not to image files linked therein. Thus images that appear on a page may not have been archived on the same date as the HTML file. Likewise, if a website is designed with "frames," the date assigned by the Internet Archive applies to the frameset as a whole, and not the individual pages within each frame.

6. Regarding archived files stored in and made available via the Wayback Machine, I further declare that:

A. to the best that the electronic systems involved can accurately record and reflect, such files were captured at or near the time of the date reflected in the URL assigned to each file by virtue of an automated transfer of electronic data;

B. such records were captured by Internet Archive or received from third party donors in the course of regularly conducted activity by the Internet Archive; and

C. the Internet Archive captures, stores, and receives from third party donors web data as a regular practice.

7. The web archives for the year 2009 in the Wayback Machine at web.archive.org were largely obtained from third-party organizations, which donated the archived data, captured by automatic electronic systems, to the Internet Archive. I do not affirm that these web archives were set forth by, or from information transmitted by, people with knowledge of the information recorded therein.

8. This document is the Internet Archive's standard affidavit, the affidavit Internet Archive normally provides to parties seeking to use Wayback Machine records as evidence in legal proceedings, with additional language provided in paragraphs 6-8.

9. Attached hereto as Exhibit A are true and accurate copies of printouts of the Internet Archive's records of the HTML files for the URLs and the dates specified in the footer of the printout.

10. I declare under penalty of perjury that the foregoing is true and correct.

The Court notes that Exhibit A contains a document entitled "Draft: The Most Wanted Leaks of 2009" that is similar to DE F but not identical as it contains additions, deletions, and changes. The URL is: [http://web.archive.org/web/200911042112937/http://WikiLeaks.org/wiki/Draft:The\\_Most\\_Wanted\\_Leaks\\_of\\_2009](http://web.archive.org/web/200911042112937/http://WikiLeaks.org/wiki/Draft:The_Most_Wanted_Leaks_of_2009). Thus, there are at least 3 versions of "Draft: The Most Wanted Leaks of 2009" available on the Internet today.

**Hearsay/Relevance** (the Court refers to PEs 31, 31A, and 31B for ID together as PE 31 for ID and refers to PEs 32, 32A, and 32B for ID as PE 32 for ID for purposes of Hearsay/Relevance findings of fact. The PE 31 and PE 32 series of exhibits are the same 2 tweets, thus hearsay/relevance findings are the same for all the exhibits in the series.

1. Defense asserts that PEs 31 and 32 for ID and PE 109 for ID are hearsay in that (1) the statement by the webpage or tweet itself is hearsay; (2) the statement of the individual who allegedly captured the site and relayed the information to archive.org or Google.cache is hearsay; and (3) the statement of archive.org or Google.cache is hearsay.

2. The Government offers PEs 31, 32, and 109 for ID not for the truth of the matters asserted within the exhibits. Rather, they offering these exhibits to show the effect that they may have had on PFC Manning. The Government asserts that, to the extent the contents of PEs 31, 32, and 109 for ID could have influenced PFC Manning, the exhibits are relevant. Defense asserts the Government has presented no evidence that PFC Manning saw or was aware of PEs 31, 32, or 109 for ID, therefore they are not relevant to any fact of consequence.

3. The Government theory of the case with respect to PE 109 for ID is that PFC Manning viewed the WikiLeaks Most Wanted List directly from the WikiLeaks webpage as depicted in PE 109 for ID on or

after 5 November 2009 not that PFC Manning viewed the list as depicted in PE 109 for ID from the archive.org website.

4. The Government has presented no forensic evidence that the tweets in PE 31 and 32 for ID or the “Most Wanted List of 2009” in PE 109 for ID were downloaded by PFC Manning. The Government has offered evidence that PFC Manning conducted searches for WikiLeaks and OpenSource.gov on Intelink; evidence of chats between PFC Manning and Press Association/Julian Assange that discussed OpenSource.gov; and evidence that when conducting searches on Intelink, when the searcher pulls up a website and proceeds to search within that website, Intelink no longer captures the search data.

#### **The Law.**

1. Evidence must be relevant to be admissible. MRE 402.
2. Evidence is relevant if it has the tendency to make a fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. MRE 401.
3. Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. MRE 801(c).
4. Hearsay evidence is inadmissible unless an exception applies or the evidence is offered for a purpose other than to prove the truth of the matter asserted. MRE 802. This rule applies to testimony given by witnesses at trial and to exhibits to the extent that exhibits contain statements.
5. Statements offered to prove the effects those statements may have had on a listener, or reader, are not offered to prove the truth of the matter asserted and, therefore, may be considered for that limited non-hearsay purpose.
6. Exhibits require authentication as a condition precedent to their admission. The requirement of authentication is satisfied by evidence sufficient to support a finding that the exhibit in question is what its proponent claims. MRE 901(a); *U.S. v. Lubich*, 72 MJ 170 (C.A.A.F. 2013).
7. Authentication is an issue of conditional relevance. MRE 104(b) and MRE 1008 govern the inquiry under MRE 901. Thus, the Court may consider only evidence offered by the proponent that is admissible at trial to make a preliminary determination whether the exhibit(s) are sufficiently authenticated for the fact-finder to make a determination that they are authentic. *Lubich*, (“MRE 901 is the same as Federal Rule of Evidence (FRE) 901 and embraces the well-established view that authentication is a component of relevancy.” And citing *U.S. v. Blanchard*, 48 M.J. 306, 309 (C.A.A.F. 1998) “federal court of appeals decisions applying these principles would be most helpful.”). FRE 901 advisory committee’s note “The requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b).” Thus, only admissible exhibits may be considered by the Court in making its preliminary determination.
8. Two methods of satisfying the authentication requirement, and the methods attempted by the Government in moving for admission of PEs 31, 31A, 31B, 32, 32A ID, and 32B are: (1) through a witness with knowledge that the exhibit is what it is claimed to be. MRE 901(b)(1) and (2) evidence of distinctive characteristics and the like. MRE 901(b)(4).

9. There are no military cases directly addressing the authentication requirements of online webpage archives. However, there are federal and state cases that have addressed authentication of online webpage archives.

a. Self Authenticated Business Record MRE 902(1)/MRE 803(6): The Government has provided no authority where a court addressing a challenge to authentication has ruled that online webpage archives from a non-government source are self-authenticating business records. The authority is to the contrary. *In re Homestore.com., Inc. v. Securities Litigation*, 340 F.Supp.2d 769 (C.D. Cal. 2004) (Printouts from a web site do not bear the indicia of reliability demanded for other self-authenticating documents under FRE 902).

b. Testimony by a Witness With Knowledge: Several federal courts have addressed challenges to authentication of archived websites by a witness with knowledge under FRE 901(b)(1). Courts addressing the issue squarely have agreed that the admission of such webpages must be predicated either upon the testimony of an employee of the archiving company or upon the testimony of someone having personal knowledge of the contents of the archived webpages such that the witness can testify that the archived copy is accurate. The only criminal case relied upon by the Government as authority to authenticate archived webpages IAW FRE 901(a)(1) is *U.S. v. Bansal*, 663 F.3d 634 (3<sup>rd</sup> Cir. 2011). In *Bansal*, the Government called a witness to testify about how the Wayback Machine website works and how reliable its contents are. The witness also compared the screenshots with previously authenticated and admitted images from the website at issue and opined based on her personal knowledge that they were authentic. The opinion did not identify who the witness was. The other two cases relied upon by the Government for the proposition that attestations by a witness with knowledge may be sufficient to authenticate archived webpages IAW FRE 901 are civil cases where confrontation is not at issue. *St. Luke's Cataract and Laser Institute, P.A. v. Sanderson*, 2006 W.L. 1320242 (M.D. Fla. 2006) and *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740 (N.D. Ill. 2004). Other courts addressing the issue include: *U.S. v. See, e.g., Sam's Riverside, Inc. v. Intercon Solutions, Inc.*, 790 F.Supp.2d 965, 980-982 (S.D. Iowa 2011) (Holding that an [archive.org](http://archive.org) employee can authenticate [archive.org](http://archive.org) webpages); *U.S. v. Shrum*, 2011 WL 1753488 at 1-3 (E.D. Arkansas 2011) (District court initially admitted [archive.org](http://archive.org) webpage sponsored by a law enforcement witness but reconsidered and excluded it. Issue was whether the curative instruction to the jury was sufficient); *Netscape Communications Corp. v. Valueclick Inc.*, 707 F.Supp.2d 640, 644 at footnote 6 (E.D. Va 2010) (District court admitted [archive.org](http://archive.org) website because sponsoring witness had seen original and could testify that the [archive.org](http://archive.org) page was an accurate copy); and *Audi AG and Volkswagen of America v. Shokan Coachworks, Inc.*, 592 F.Supp.2d 246, 278 (N.D. New York 2008) ("Defendants correctly point out that the Adams Declaration cannot authenticate the search results from [www.archive.org](http://www.archive.org) because such evidence may only be authenticated by a knowledgeable employee of the website.").

c. The only case presented to the Court by the parties that directly addresses authentication IAW FRE 901(a)(1) where a third party has donated an archived webpage to [archive.org](http://archive.org) is a civil case, *Novak v. Tucow's, Inc.*, 2007 U.S. Dist. LEXIS 21269 (E.D.N.Y. 2007), *aff'd* 330 Fed. Appx. 204 (2<sup>nd</sup> Cir. 2009) (the information at issue was only as reliable as the third-party donor made it.)

10. The Court considers issues of hearsay and whether evidence should be excluded under MRE 403 as preliminary questions IAW MRE 104(a).

#### **Conclusions of Law Authentication:**

1. The Court will consider only admissible evidence offered by the proponent that will go before the fact-finder in making a preliminary determination regarding authentication.

2. PE 31, 31A, 31B, 32, 32A, and 32B for ID have been properly authenticated IAW MRE 901(b)(1) via the testimony of SA Mander. Although PE 31 and 32 for ID are retrieved from Google.cache, SA Mander testified that he retrieved copies of the same tweets directly from twitter.com as PE 31A and B and PE 32A and B. These exhibits are also properly authenticated IAW MRE 901(b)(4) distinctive characteristics as set forth in the Court's findings of fact regarding these exhibits. PE 31, 31A, 31B, 32, 32A, and 32B for ID are properly authenticated.

3. PE 109 for ID is not sufficiently reliable to be a self-authenticating business record IAW MRE 902(11) and MRE 803(6). For authentication IAW MRE 901, federal case law on the authentication issue is persuasive. A witness sponsoring the admission of archived webpages must either have knowledge of the archiving procedures used by the archiving entity and/or third party donor entity such that the witness can testify that the archive actually shows true copies of the websites they purport to archive or must have knowledge of the original webpage such that the witness can verify that the archived copy is a true copy of the original. The Government has advised the Court that it does not intend to admit the attestation by Mr. Butler (enclosure 1 of the Government's brief). Accordingly, this court finds that the Government has not properly authenticated PE 109 for ID and it is not admitted.

4. The PE 31 series of exhibits provide evidence that WikiLeaks or an entity purporting to be WikiLeaks posted a tweet on 7 May 2010, requesting a list of as many .mil email addresses as possible. The PE 31 series of exhibits is offered by the Government for non-hearsay purposes. PE 31 series of exhibits is offered as circumstantial evidence to show PFC Manning's intent to respond to WikiLeaks queries and his knowledge of the scope of disclosures WikiLeaks intended to make. The Government has introduced forensic evidence from SA Al Williamson that the accused downloaded the U.S. forces-Iraq Microsoft Outlook/Share-point Exchange Server global address list (GAL) between 11-27 May 2010. This evidence is relevant to the specification of Charge I (Aiding the Enemy) and specification 16 of Charge II (stealing, purloining, or knowingly converting the GAL between on or about 11 -27 May 2010).

5. The 8 January 2010 tweet in PE 32 series of exhibits states "Have encrypted videos of US bomb strikes on civilians <http://bit.ly/wlafghan2> we need supercomputer time <http://ljsf.org/>." The portion of the tweet stating "Have encrypted videos of U.S. bomb strike on civilians." is a statement. The Government offers the tweet (1) as a hearsay exception under MRE 803(3) (then existing state of mind) to demonstrate WikiLeaks publicized plan to compromise military information as of 8 January 2010; (2) for the non-hearsay purpose to show PFC Manning's awareness of WikiLeaks' openly and publicly posted plan to disclose classified information; (3) for the non-hearsay purpose of the publication of the tweet looking for assistance to unencrypt the video as circumstantial evidence to connect the timing of the tweet to the appearance on Mr. Jason Katz' computer on 15 December 2009 of an Afghan video with the same hash values as the Afghan video from the CENTCOM server allegedly communicated to WikiLeaks by PFC Manning; and (4) as a hearsay exception under MRE 803(3) to corroborate PFC Manning's admissions that he sent WikiLeaks an encrypted video in the internet chats. For the reasons proffered by the Government above PE 32 is relevant as evidence of PFC Manning's knowledge of the scope of WikiLeaks' intended disclosure for the specification of Charge I (Aiding the Enemy), specification 1 of Charge II (Wantonly Causing to be Published) and to prove willful communication of the Gharani video for specification 11 of Charge II.

6. PE 109 for ID is a request for information and is offered for the fact that the request was made not for the truth of the matter asserted. The Government offers PE 109 for ID for a non-hearsay purpose as circumstantial evidence that PFC Manning was aware of PE 109 for ID and his intent to gather information and send it to WikiLeaks. Although the Government has not presented evidence that the accused actually accessed PE 109 for ID, the Government has presented evidence that PFC Manning searched Intelink for WikiLeaks and for some of the information on PE 109 for ID. The Government also

presented evidence that when a person does an Intelink search and navigates to another website to continue the search, Intelink no longer captures the meta-data. The Court finds timing of the PE 109 for ID posting in conjunction with other evidence presented by the Government is relevant circumstantial evidence offered for a non-hearsay purpose to further the inference that PFC Manning was aware of the information requested by WikiLeaks in PE 109 for ID. Should PE 109 for ID be properly authenticated, it is relevant for the specifications in Charges I and II.

7. The Court has considered whether the probative value of PE 31 and 32 for ID series of exhibits is substantially outweighed by the danger of unfair prejudice under the criteria in MRE 403 and finds it is not. The Court as fact-finder will consider the evidence for the proper admissible purposes.

**RULING:** The Government motion to admit PEs 31, 31A, 31B, 32, 32A, and 32B for ID is **GRANTED**. The Government motion to admit PE 109 for ID is **DENIED**.

So **ORDERED** this 28<sup>th</sup> day of June 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
U.S. ARMY MILITARY DISTRICT OF WASHINGTON  
210 A STREET  
FORT LESLEY J. MCNAIR, DC 20319-5013

June 28, 2013

Criminal Law Division, Office of the Staff Judge Advocate

Mr. Christopher Butler  
Internet Archive  
300 Funston Avenue  
San Francisco, CA 94118

Re: United States v. Private First Class (PFC) Bradley Manning

Dear Mr. Butler or an alternate Records Custodian:

This office respectfully requests prompt compliance with the enclosed Subpoena in the above-referenced U.S. Army court-martial. The below documents are being requested for you to bring with you to Fort Meade, Maryland.

1. All documents related to the following URL:  
"http://web.archive.org/web/20091105061330/http://wikileaks.org/wiki/Draft:The\_Most\_Wanted\_Leaks\_of\_2009-sort".
2. All documents related to the following URL:  
"http://web.archive.org/web/20091104212937/http://wikileaks.org/wiki/Draft:The\_Most\_Wanted\_Leaks\_of\_2009".
3. All documents related to whether the above listed URLs were collected or archived by web.archive.org.
4. All documents related to whether the above listed URLs were obtained or donated from third-party organizations, and if so, which organization donated the URLs.

This criminal trial is currently in progress. I request that you produce the above listed records when you arrive to the courthouse on July 1, 2013. These records will be used in trial. You may comply with this order by signing the enclosed subpoena and returning it to the servicing agent. Please contact our travel section as soon as possible at 202-685-1975, or by email at [usarmy.mcnair.mdw.mbx.witness@mail.mil](mailto:usarmy.mcnair.mdw.mbx.witness@mail.mil). This office will fund all reasonable costs directly associated with your travel. I greatly appreciate your assistance and cooperation.

Sincerely,

Ashden Fein  
Major, U.S. Army  
Trial Counsel

Enclosure

APPELLATE EXHIBIT 585  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES



**SUBPOENA**

The President of the United States, to \_\_\_\_\_ Mr. Christopher Butler or an alternate Records Custodian  
*(Name and Title of Person being Subpoenaed)*

You are hereby summoned and required to appear on the \_\_\_\_\_ 1st day of \_\_\_\_\_ July \_\_\_\_\_, 2013, at 7:00 o'clock \_\_\_\_\_ A.M., at Fort Meade, Maryland \_\_\_\_\_, (before \_\_\_\_\_  
*(Place of Proceeding) (Name and Title of Deposition Officer)*)  
designated to take your deposition) (a General court-martial of the United States) (a court of inquiry), appointed by \_\_\_\_\_ Court-Martial Convening Order Number I \_\_\_\_\_, dated 11 February \_\_\_\_\_,  
*(Identification of Convening Order or Convening Authority)*  
2012, to testify as a witness in the matter of \_\_\_\_\_ United States v. Private First Class (PFC) Bradley Manning \_\_\_\_\_,  
*(Name of Case)*  
(and bring with you \_\_\_\_\_ the documents referenced in the enclosed cover letter \_\_\_\_\_).  
*(Specific Identification of Documents or Other Evidence)*

Failure to appear and testify is punishable by a fine of not more than \$500 or imprisonment for a period not more than six months, or both. (10 U.S.C. §847). Failure to appear may also result in your being taken into custody and brought before the court-martial ( \_\_\_\_\_ US v. PFC Manning \_\_\_\_\_ ) under a Warrant of Attachment (DD Form 454) Manual for Courts-Martial R.C.M. 703(e)(2)(G).

Bring this subpoena with you and do not depart from the proceeding without proper permission

Subscribed at \_\_\_\_\_ Fort Meade, Maryland \_\_\_\_\_ this 28th day of \_\_\_\_\_ June \_\_\_\_\_, 2013.  
\_\_\_\_\_  
*(Signature (See R.C.M. 703 (e)(2)(C))*

The witness is requested to sign one copy of this subpoena and to return the signed copy to the person serving the subpoena.

I hereby accept service of the above subpoena. \_\_\_\_\_  
*Signature of Witness*

**NOTE:** If the witness does not sign, complete the following:  
Personally appeared before me, the undersigned authority, Tabitha L. Stires, who, being first duly sworn according to law, deposes and says that at 1500 PT. 28 June, 2013, he personally delivered to Christopher Butler in person a duplicate of this subpoena.

\_\_\_\_\_  
*Grade*

Subscribed and sworn to before me at \_\_\_\_\_, this \_\_\_\_\_ day of \_\_\_\_\_.

\_\_\_\_\_  
*Grade*

**Investigative Operations Analyst Tabitha L. Stires**  
*Official Status Signature*

**Ford, Arthur D Jr CW2 USARMY (US)**

---

**From:** Hanni Fakhoury [hanni@eff.org]  
**Sent:** Friday, June 28, 2013 7:46 PM  
**To:** Ford, Arthur D Jr CW2 USARMY (US)  
**Cc:** Nate Cardozo; Kurt Opsahl  
**Subject:** 6.28.13 Subpoena to Internet Archive

Chief Warrant Officer Ford,

The Electronic Frontier Foundation represents the Internet Archive with respect to the June 28, 2013 subpoena it received, requesting records and testimony at Fort Meade on Monday July 1, 2013 at 7:00 a.m.

As I explained over the phone, the Archive intends to comply with the subpoena but cannot do so in the specified time frame. Because the documents cannot be prepared by the requested time, the Archive needs additional time to comply.

Specifically, the Archive requests a delay until the week of July 8 to produce the records and appear at Fort Meade.

Feel free to email or call the number below at your convenience if there are any other questions I can answer for you.

Thanks,

Hanni M. Fakhoury  
Staff Attorney  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
415 436 9333 x. 117

[hanni@eff.org](mailto:hanni@eff.org)  
[www.eff.org](http://www.eff.org)

On Twitter @hannifakhoury  
EFF blog: <https://www.eff.org/about/staff/hanni-fakhoury>

Help EFF Defend Freedom in the Digital World <https://www.eff.org/donate>

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

RELEVANCE AND NON-HEARSAY  
PURPOSE FOR FACTS TO  
BE JUDICIALLY NOTICED

28 June 2013

The United States provides the following statement to the defense and Court in support of its request for judicial notice of certain adjudicative facts:

**Julian Assange was located in Iceland in February of 2010 and working on the Icelandic Modern Media Initiative. See AE 472.**

The Government has presented evidence that PFC Manning searched on Intelink for "Iceland" and "wikileaks." The defense stipulated to this fact during the testimony of Mr. Chad Madaras. The Government presented evidence that PFC Manning searched the Open Source Center for "Iceland" and "wikileaks" on 20 February 2010. The Government presented evidence that PFC Manning and the "pressassociation" account – associated with Julian Assange – discussed topics related to WikiLeaks, the Icelandic Modern Media Initiative (IMMI), and Iceland generally in the March 2010 timeframe. This fact is relevant as it provides context to the nature of the chats between PFC Manning and "pressassociation." This fact is also relevant to PFC Manning's knowledge and relationship to WikiLeaks and Assange, and whether PFC Manning acted "wantonly" and "caused to be published" intelligence information on the internet, two elements of Specification 1 of Charge II.


**That LTC Lee Packnett was quoted in a New York Times article, dated 18 March 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. See AE 472.**

The Government presented evidence that PFC Manning and Julian Assange discussed LTC Packnett being quoted in a New York Times article in the March 2010 timeframe. This fact is relevant as it provides context to the nature of the chats between PFC Manning and "pressassociation." The date of the New York Times article is not hearsay as it is not a statement. The fact that the article exists and that LTC Packnett is quoted is not hearsay as it is not a statement. This adjudicative fact is relevant to PFC Manning's knowledge and relationship with WikiLeaks and Assange, facts that tend to show that PFC Manning acted "wantonly" and "caused to be published" intelligence information on the internet, two elements of Specification 1 of Charge II.


**That a New Yorker profile of Julian Assange, titled "No Secrets: Julian Assange's Mission for Total Transparency" exists and was dated 7 June 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. See AE 472.**

APPELLATE EXHIBIT 587  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

The Government presented evidence that PFC Manning and Mr. Adrian Lamo discussed a New Yorker profile of Julian Assange in late May 2010. The fact that PFC Manning knew about the New Yorker article prior to the date of publication is relevant to show the extent of PFC Manning's knowledge and relationship with WikiLeaks and Assange, facts that are relevant to whether PFC Manning "caused to be published" intelligence information on the internet, an element of Specification 1 of Charge II. The date of the New Yorker profile of Julian Assange (7 June 2010) is not hearsay as it is not a statement.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on defense counsel, via electronic mail, on 28 June 2013.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**RELEVANCE AND NON-HEARSAY  
PURPOSE FOR FACTS TO  
BE JUDICIALLY NOTICED**

28 June 2013

The United States provides the following statement to the defense and Court in support of its request for judicial notice of certain adjudicative facts:

Julian Assange was located in Iceland in February of 2010 and working on the Icelandic Modern Media Initiative. *See* AE 472.

[The Government has presented evidence that PFC Manning searched on Intelink for "Iceland" and "wikileaks". The defense stipulated to this fact during the testimony of Mr. Chad Madaras. [The Government presented evidence that PFC Manning searched the Open Source Center for "Iceland" and "wikileaks" on 20 February 2010. [The Government presented evidence that PFC Manning and the "pressassociation" account – associated with Julian Assange – discussed topics related to WikiLeaks, the Icelandic Modern Media Initiative (IMMI), and Iceland generally in the March 2010 timeframe.] This fact is relevant as it provides context to the nature of the chats between PFC Manning and "pressassociation." This fact is also relevant to PFC Manning's knowledge and relationship to WikiLeaks and Assange, and whether PFC Manning acted "wantonly" and "caused to be published" intelligence information on the internet, two elements of Specification 1 of Charge II.

**Comment [A1]:** PE 81 at lines 76, 185, 324, 327, 328, 341. The United States can provide additional line references if needed.

**Comment [A2]:** Testimony of SA Shaver

**Comment [A3]:** PE 123 at 1 (21:09:27), 3 (07:20:54), 4 (06:05:22), 5 (06:16:34), 8 (06:04:02), 9 (21:10:31).

That LTC Lee Packnett was quoted in a New York Times article, dated 18 March 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *See* AE 472.

[The Government presented evidence that PFC Manning and Julian Assange discussed LTC Packnett being quoted in a New York Times article in the March 2010 timeframe. This fact is relevant as it provides context to the nature of the chats between PFC Manning and "pressassociation." The date of the New York Times article is not hearsay as it is not a statement. The fact that the article exists and that LTC Packnett is quoted is not hearsay as it is not a statement. This adjudicative fact is relevant to PFC Manning's knowledge and relationship with WikiLeaks and Assange, facts that tend to show that PFC Manning acted "wantonly" and "caused to be published" intelligence information on the internet, two elements of Specification 1 of Charge II.

**Comment [A4]:** PE 123 at 12 (08:42:06)


That a New Yorker profile of Julian Assange, titled "No Secrets: Julian Assange's Mission for Total Transparency" exists and was dated 7 June 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *See* AE 472.

The Government presented evidence that PFC Manning and Mr. Adrian Lamo discussed a New Yorker profile of Julian Assange in late May 2010. The fact that PFC Manning knew about the New Yorker article prior to the date of publication is relevant to show the extent of PFC Manning's knowledge and relationship with WikiLeaks and Assange, facts that are relevant to whether PFC Manning "caused to be published" intelligence information on the internet, an element of Specification 1 of Charge II. The date of the New Yorker profile of Julian Assange (7 June 2010) is not hearsay as it is not a statement.

Comment [AS]: PE 30 at 19 (1028:21 AM).  
Testimony of SA Shaver and Adrian Lamo (chat took place in late May 2010).

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on defense counsel, via electronic mail, on 28 June 2013.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Combined Judicial Notice

28 June 2013

I. Reference Materials

A. The Court took judicial notice that the existence and the content of following reference materials are adjudicative facts:

1. Army Regulation (AR) 25-2, paras 1-4, 1-5, 3-3, 4-5, 4-16, 4-17, and Figure B 1. *See* Appellate Exhibit (AE) 288; AE 248.

2. AR 380-5, paras 1-20, 1-21, 1-22 and Chapters 2, 4 (Section 1), 5 (Sections I and V), and paras 6-1, 6-2, 6-3, 7-4, 8-3, and 8-12. *Id.*

3. AR 530-1, paras 1-5, 1-6, 1-7, and 2-1. *Id.*

4. 18 U.S.C. §793(e). *Id.*

5. 18 U.S.C. §1030(a). *Id.*

6. 18 U.S.C. §641. *Id.*

7. Executive Order (EO) 13526. *Id.*

8. Authorization for the Use of Military Force. *Id.*

9. July 2011 Information Paper by HQDA DCS, G-2, Initiatives Group (DIG). *See* AE 288; AE 233, Attachment A.

10. Commander's Handbook Distributed Common Ground System – Army DCGS-A, March 30, 2009. *See* AE 288; AE 233, Attachment B.

11. EO 12958. *See* AE 472.

12. EO 12972. *Id.*

13. EO 13142. *Id.*

14. EO 13292. *Id.*

APPELLATE EXHIBIT 588  
PAGE RE-ENTERED  
PAGE 588 PAGES

15. Public Law 111-258. AE 481.

16. AR 25-1, paras 1-1, 1-7(a) and (b), and 6-1 (d) –(f). *See* AE 582.

17. AR 25-2 definition of “Information System”. *Id.*

18. Department of Defense Regulation 5400.11-R, Appendix 1 and the definition of “Personal Information”. *Id.*

B. The Court will take judicial notice of the existence and the content of the following reference materials, conditional on the relevance of these materials:

1. Army Field Manual 2-0 “Intelligence”. *See* AE 472.

2. Army Field Manual 2-19.4 “Brigade Combat Team Intelligence Operations”. *Id.*

3. Army Field Manual 2-22.2 “Counterintelligence”. *Id.*

4. Army Field Manual 2-22.3 “Human Intelligence Collector Operations”. *Id.*

5. Army Soldier’s Manual and Trainer’s Guide for Intelligence Analysis MOS 35F, Skill Level 1/2/3/4. *Id.*

6. Court will take judicial notice of the findings in Section 2 of PL 111-258 to the degree they are relevant. Such judicial notice would be the adjudicative fact that Congress made the findings (that Congress believed over-classification was a potential issue and passed this legislation – which contains not just findings but specific statutory initiatives – to address that issue), not that the findings by Congress are adjudicative fact. Thus, subject to a demonstration of relevance, the Court will take judicial notice of the existence of PL 111-258, to include the Congressional finding in Section 2, the date of introduction of H.R. 255 and the date the law was enacted. The Court will not take judicial notice of the truth of the matter asserted in PL 111-258 as adjudicative facts. AE 481.

## II. Statements, Articles, and Print Material

A. The Court took judicial notice of the following facts associated with statements, articles, and print material:

1. That the 13 October 2010 classification assessment by RADM Donegan exists and that RADM Donegan gave this assessment. This information is admissible as an admission of a party opponent under MRE 801(d)(2)(D), given he was acting in his official capacity as Direct of Operations, CENTCOM, when he made the classification assessment and that the assessment states facts inconsistent with the Stipulation of Expected Testimony of CW5 John Larue at PE 117. *See* AE 582.



2. The audio transcript for PE 15. *Id.* The parties stipulate that Enclosure 2 to AE 574 is an accurate transcript of the audio in PE 15.

B. The Court took judicial notice of the following facts associated with statements, articles, and print material for pre-sentencing only:

1. That the Advanced Ace, Advanced Analytical, Capability Joint Urgent Operation Need Statement, MG Michael T Flynn, Deputy Chief of Staff Intelligence 2 July 2010 exists. *See* AE 288; AE 233, Attachment C.

2. That the letter regarding global knowledge management dated 19 July 2010 from three members of Congress to the Chairman and ranking members of the House Appropriations Committee exists. *See* AE 288; AE 233, Attachment D.

3. That the letter to the Chairman of the House Appropriations Committee from COL Peter A. Newell, Director, Rapid Equipping Force, dated 28 July 2010, exists. *See* AE 288; AE 233, Attachment E.

4. That the letter to COL Newell from members of Congress Gabrielle Giffords and Adam Smith, dated 25 August 2011, exists. *See* AE 288; AE 233, Attachment F.

5. That the letter from Adam Smith, Congress member, to General Dempsey, dated 23 May 2011, exists. *See* AE 288; AE 233, Attachment G.

6. That a Department of Defense news Release entitled "Statement by Pentagon Press Secretary Geoff Morrell and Special Envoy for Closure of Guantanamo Detention Facility Ambassador Daniel Fried", dated 24 April 2011, exists and that Mr. Morrell made these statements. The statements are admissible under MRE 801(d)(2)(D). *See* AE 356; AE 316.

7. That a White House release entitled "Remarks by the President After Bipartisan Leadership Meeting", dated 27 July 2010, exists and that President Obama made these statements. The statements are admissible under MRE 801(d)(2)(D). *Id.*

8. That a letter to Secretary Robert Gates from Carl Levin, dated 28 July 2010, exists. ~~The statements are admissible under MRE 801(d)(2)(D) and MRE 803(8)(A).~~ *Id.*

9. That a letter to Carl Levin from Robert Gates, dated 16 August 2010, exists. The statements are admissible under MRE 801(d)(2)(D) and MRE 803(8)(A). *Id.*

10. That a news release entitled "DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon", dated 30 November 2010, exists and that Secretary Gates made these statements. Admissible for non-hearsay purpose as public statements made by government officials that provide circumstantial evidence of minimized damage cause by the alleged Wikileaks disclosures. *Id.*

11. That Department of State-published remarks entitled "Remarks with Kazakh Foreign Minister Saudabayev after their Meeting", dated 1 December 2010, exist and that Secretary Clinton made these statements. Admissible for non-hearsay purpose as public statements made by government officials that provide circumstantial evidence of minimized damage cause by the alleged Wikileaks disclosures. *Id.*

12. William Leonard, Director of Information Security Oversight Office of the National Archive, statements, dated 22 March 2007 given at the 2007 House Committee on Homeland Security Hearings.

C. The Court will take judicial notice of the below-listed facts associated with statements, articles, and print material, conditional on the following:

1. That LTC Lee Packnett was quoted in a New York Times article, dated 18 March 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *See* AE 472.

2. That a New Yorker profile of Julian Assange, titled "No Secrets: Julian Assange's Mission for Total Transparency" exists and was dated 7 June 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *Id.*

3. David Finkel's book "The Good Soldiers" exists. AE 356. The Court will take judicial notice the date of publication, and the provided excerpts. AE 356. Comparisons between Mr. Finkel's book and conclusions to be drawn from the comparisons are properly presented to the fact finder by the parties not by the Court. The request to take judicial notice that the book quotes the video verbatim at several key points is denied. AE 356. Linkages, argument, and legal conclusions regarding the contents of Mr. Finkel's book and the audio in the video are properly presented to the fact finder by the parties. *See* AE 288.

D. The Court will take judicial notice of the below-listed facts associated with statements, articles, and print material, for pre-sentencing only, conditional on the following:

1. That a UPI News Track news story entitled "Clinton on Leaked Documents: So What?", dated 4 December 2010, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *See* AE 356; AE 316.

2. That a New York Times news story entitled "From WikiLemons, Clinton Tries to make Lemonade", dated 4 December 2010, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *See* AE 356; AE 316.

3. That a CNN news story entitled "Clinton: WikiLeaks Cables Show Diplomacy at Work", dated 4 December 201, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *Id.*

4. That an interview described on MSNBC entitled “Biden on Start, WikiLeaks” exists. In this instance, judicial notice is conditional on the defense providing the Court with the date of this interview. *Id.*

5. The 22 March 2007 testimony of Mr. Leonard is admissible under MRE 803(8)(A) if relevant. AE 481. The key assertion cited by the Defense, that trained government classifiers only made “clearly” correct classification decisions 64 percent of the time was based on an official audit. (“In an audit of agency classification activity conducted by my office approximately one year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it right only 64 percent of the time in making determinations as to the appropriateness of classification.”).

### III. Historical Facts

A. The Court took judicial notice of the following historical facts:

1. WikiLeaks and various news organizations began publishing purported Department of State diplomatic cables over the weekend of 27-28 November 2010. *See* AE 472.

2. On 19 January 2010, the Department of State listed “al-Qa’ida in the Arabian Peninsula” (AQAP) as a foreign terrorist organization. Since that date, AQAP has been an enemy of the United States. *See* AE 472.

3. Usama bin Laden was a member of Al-Qaeda (AQ) and an enemy of the United States. *See* AE 472.

4. Adam Gadahn is a member of AQ and an enemy of the United States. *See* AE 472.

5. David Finkel’s book “The Good Soldiers” was published prior to the alleged leaks in this case. *See* AE 288.

6. There has been consistent and extensive media coverage of this case. *See* AE 283.

7. WikiLeaks released a video titled “Collateral Murder” on 5 April 2010. *See* AE 582.

8. WikiLeaks released more than 390,000 records from the Combined Information Data Network Exchange (CIDNE) Iraq database on 22 October 2010. *Id.*

9. Wikileaks released more than 75,000 records from the CIDNE Afghanistan database on 25 July 2010. *Id.*

10. WikiLeaks released more than 700 detainee assessments produced by Joint Task Force Guantanamo (JTF-GTMO) on 25 April 2011. *Id.*

11. WikiLeaks released a memorandum produced by the Army Counterintelligence Center titled "WikiLeaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 15 March 2010. *Id.*

12. The monthly base salary for Servicemembers at the rank of Specialist, E-4, was \$1,502.70 in 2003, \$1,558.20 in 2004, \$1,612.80 in 2005, \$1,662.90 in 2006, \$1,699.50 in 2007, \$1,758.90 in 2008, \$1,827.60 in 2009, and \$1,889.70 in 2010. *Id.*

13. The yearly base salary for government employees at the grade of 12 on the General Schedule (GS) scale was \$51,508 in 2003; \$52,899 in 2004; \$54,221 in 2005, \$55,360 in 2006, \$56,301 in 2007, \$57,709 in 2008, \$59,383 in 2009, and \$60,274 in 2010. *Id.*

14. Thanksgiving of 2009 occurred on 26 November 2009. *Id.*

15. The term ".is" is the top level internet domain of Iceland. *Id.*

16. Johanna Sigurdardottir was the Prime Minister of Iceland from February 2009 – May 2013. *Id.*

17. Ossur Skarphedinsson was the Icelandic Minister for Foreign Affairs from February 2009- May 2013. *Id.*

18. Albert Jonsson was the Icelandic Ambassador to the United States 2006-2009. *Id.*

19. Birgitta Jonsdottir has been a member of the Icelandic parliament since 2009. *Id.*

20. On or about 25 November 2009, WikiLeaks published what it claimed to be text and pager messages sent on 11 September 2001. Judicial notice does not extend to the content of the messages or that the messages are actually from 11 September 2001. *Id.*

21. On 25 July 2007, Reuters made a FOIA request to DoD for video and audio recordings relating to the deaths of Mr. Namir Noor-Eldeen and Mr. Saeed Chmagh, Reuters journalists. CENTCOM responded to the Reuters request on 24 April 2009. *Id.*

B. The Court took judicial notice of the following historical facts for the presentencing phase of proceedings:

1. Damage Assessments exist. *See* AE 472.

2. The Office of National Counterintelligence Executive, the Information Review Task Force, and the Department of States created or compiled their respective damage assessments on the noted dates. *Id.*

3. The Department of State damage assessment is the most current version and is a draft. *Id.*

C. The Court will take judicial notice of the following historical facts, conditional on the relevance of these materials:

1. Julian Assange was located in Iceland in February of 2010 and working on the Icelandic Modern Media Initiative. *See* AE 472.

2. "Inspire" is a magazine. *Id.*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Combined Judicial Notice

1 July 2013

## I. MERITS

A. The Court took judicial notice of the following adjudicative facts for the merits:

1. Army Regulation (AR) 25-2, paras 1-4, 1-5, 3-3, 4-5, 4-16, 4-17, and Figure B 1. *See* Appellate Exhibit (AE) 288; AE 248.

2. AR 380-5, paras 1-20, 1-21, 1-22 and Chapters 2, 4 (Section 1), 5 (Sections I and V), and paras 6-1, 6-2, 6-3, 7-4, 8-3, and 8-12. *Id.*

3. AR 530-1, paras 1-5, 1-6, 1-7, and 2-1. *Id.*

4. 18 U.S.C. §793(e). *Id.*

5. 18 U.S.C. §1030(a). *Id.*

6. 18 U.S.C. §641. *Id.*

7. Executive Order (EO) 13526. *Id.*

8. Authorization for the Use of Military Force. *Id.*

9. July 2011 Information Paper by HQDA DCS, G-2, Initiatives Group (DIG). *See* AE 288; AE 233, Attachment A.

10. Commander's Handbook Distributed Common Ground System – Army DCGS-A, March 30, 2009. *See* AE 288; AE 233, Attachment B.

11. EO 12958. *See* AE 472.

12. EO 12972. *Id.*

13. EO 13142. *Id.*

14. EO 13292. *Id.*

15. AR 25-1, paras 1-1, 1-7(a) and (b), and 6-1 (d)-(f). *See* AE 582.

16. AR 25-2 definition of "Information System." *Id.*

17. Department of Defense Regulation 5400.11-R, Appendix 1 and the definition of "Personal Information." *Id.*

18. That the 13 October 2010 classification assessment by RADM Donegan exists and that RADM Donegan gave this assessment. This information is admissible as an admission of a party opponent under MRE 801(d)(2)(D), given he was acting in his official capacity as Direct of Operations, CENTCOM, when he made the classification assessment and that the assessment states facts inconsistent with the Stipulation of Expected Testimony of CW5 John Larue at PE 117. *See* AE 582.

19. The audio transcript for PE 15. *Id.* The parties stipulate that Enclosure 2 to AE 574 is an accurate transcript of the audio in PE 15.

20. David Finkel's book "The Good Soldiers" was published prior to the alleged leaks in this case. *See* AE 288.

21. David Finkel's book "The Good Soldiers" exists. AE 356. The Court will take judicial notice the date of publication, and the provided excerpts. AE 356. Comparisons between Mr. Finkel's book and conclusions to be drawn from the comparisons are properly presented to the fact finder by the parties not by the Court. The request to take judicial notice that the book quotes the video verbatim at several key points is denied. AE 356. Linkages, argument, and legal conclusions regarding the contents of Mr. Finkel's book and the audio in the video are properly presented to the fact finder by the parties. *See* AE 288.

22. WikiLeaks and various news organizations began publishing purported Department of State diplomatic cables over the weekend of 27-28 November 2010. *See* AE 472.

23. On 19 January 2010, the Department of State listed "al-Qa'ida in the Arabian Peninsula" (AQAP) as a foreign terrorist organization. Since that date, AQAP has been an enemy of the United States. *See* AE 472.

24. Usama bin Laden was a member of Al-Qaeda (AQ) and an enemy of the United States. *See* AE 472.

25. Adam Gadahn is a member of AQ and an enemy of the United States. *See* AE 472.

26. There has been consistent and extensive media coverage of this case. *See* AE 283.

27. WikiLeaks released a video titled "Collateral Murder" on 5 April 2010. *See* AE 582.

28. WikiLeaks released more than 390,000 records from the Combined Information Data Network Exchange (CIDNE) Iraq database on 22 October 2010. *Id.*

29. Wikileaks released more than 75,000 records from the CIDNE Afghanistan database on 25 July 2010. *Id.*

30. WikiLeaks released more than 700 detainee assessments produced by Joint Task Force Guantanamo (JTF-GTMO) on 25 April 2011. *Id.*

31. WikiLeaks released a memorandum produced by the Army Counterintelligence Center titled "WikiLeaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 15 March 2010. *Id.*

32. The monthly base salary for Servicemembers at the rank of Specialist, E-4, was \$1,502.70 in 2003, \$1,558.20 in 2004, \$1,612.80 in 2005, \$1,662.90 in 2006, \$1,699.50 in 2007, \$1,758.90 in 2008, \$1,827.60 in 2009, and \$1,889.70 in 2010. *Id.*

33. The yearly base salary for government employees at the grade of 12 on the General Schedule (GS) scale was \$51,508 in 2003; \$52,899 in 2004; \$54,221 in 2005, \$55,360 in 2006, \$56,301 in 2007, \$57,709 in 2008, \$59,383 in 2009, and \$60,274 in 2010. *Id.*

34. Thanksgiving of 2009 occurred on 26 November 2009. *Id.*

35. The term ".is" is the top level internet domain of Iceland. *Id.*

36. Johanna Sigurdardottir was the Prime Minister of Iceland from February 2009-May 2013. *Id.*

37. Ossur Skarphedinsson was the Icelandic Minister for Foreign Affairs from February 2009-May 2013. *Id.*

38. Albert Jonsson was the Icelandic Ambassador to the United States 2006-2009. *Id.*

39. Birgitta Jonsdottir has been a member of the Icelandic parliament since 2009. *Id.*

40. On or about 25 November 2009, WikiLeaks published what it claimed to be text and pager messages sent on 11 September 2001. Judicial notice does not extend to the content of the messages or that the messages are actually from 11 September 2001. *Id.*

41. On 25 July 2007, Reuters made a FOIA request to DoD for video and audio recordings relating to the deaths of Mr. Namir Noor-Eldeen and Mr. Saeed Chmagh, Reuters journalists. CENTCOM responded to the Reuters request on 24 April 2009. *Id.*

B. The Court will take judicial notice on the merits, conditional on the following:

1. That LTC Lee Packnett was quoted in a New York Times article, dated 18 March 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *See* AE 472.



2. That a New Yorker profile of Julian Assange, titled "No Secrets: Julian Assange's Mission for Total Transparency" exists and was dated 7 June 2010. In this instance, judicial notice is conditional upon relevance and a non-hearsay or hearsay exception usage. *Id.*

3. Julian Assange was located in Iceland in February of 2010 and working on the Icelandic Modern Media Initiative. *See* AE 472. In this instance, judicial notice is conditional upon relevance.

4. Army Field Manual 2-0 "Intelligence." *See* AE 472. In this instance, judicial notice is conditional upon relevance.

5. Army Field Manual 2-19.4 "Brigade Combat Team Intelligence Operations." *Id.* In this instance, judicial notice is conditional upon relevance.

6. Army Field Manual 2-22.2 "Counterintelligence." *Id.* In this instance, judicial notice is conditional upon relevance.

7. Army Field Manual 2-22.3 "Human Intelligence Collector Operations." *Id.* In this instance, judicial notice is conditional upon relevance.

8. Army Soldier's Manual and Trainer's Guide for Intelligence Analysis MOS 35F, Skill Level 1/2/3/4. *Id.* In this instance, judicial notice is conditional upon relevance.

## II. PRE-SENTENCING

A. For pre-sentencing proceedings, the Court took judicial notice of the following:

1. Public Law 111-258.

2. That the Advanced Ace, Advanced Analytical, Capability Joint Urgent Operation Need Statement, MG Michael T Flynn, Deputy Chief of Staff Intelligence 2 July 2010 exists. *See* AE 288; AE 233, Attachment C.

3. That the letter regarding global knowledge management dated 19 July 2010 from three members of Congress to the Chairman and ranking members of the House Appropriations Committee exists. *See* AE 288; AE 233, Attachment D.

4. That the letter to the Chairman of the House Appropriations Committee from COL Peter A. Newell, Director, Rapid Equipping Force, dated 28 July 2010, exists. *See* AE 288; AE 233, Attachment E.

5. That the letter to COL Newell from members of Congress Gabrielle Giffords and Adam Smith, dated 25 August 2011, exists. *See* AE 288; AE 233, Attachment F.

6. That the letter from Adam Smith, Congress member, to General Dempsey, dated 23 May 2011, exists. *See* AE 288; AE 233, Attachment G.

7. That a Department of Defense news Release entitled "Statement by Pentagon Press Secretary Geoff Morrell and Special Envoy for Closure of Guantanamo Detention Facility Ambassador Daniel Fried", dated 24 April 2011, exists and that Mr. Morrell made these statements. The statements are admissible under MRE 801(d)(2)(D). *See* AE 356; AE 316.

8. That a White House release entitled "Remarks by the President After Bipartisan Leadership Meeting", dated 27 July 2010, exists and that President Obama made these statements. The statements are admissible under MRE 801(d)(2)(D). *Id.*

9. That a letter to Secretary Robert Gates from Carl Levin, dated 28 July 2010, exists.

10. That a letter to Carl Levin from Robert Gates, dated 16 August 2010, exists. The statements are admissible under MRE 801(d)(2)(D) and MRE 803(8)(A). *Id.*

11. That a news release entitled "DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon", dated 30 November 2010, exists and that Secretary Gates made these statements. Admissible for non-hearsay purpose as public statements made by government officials that provide circumstantial evidence of minimized damage cause by the alleged Wikileaks disclosures. *Id.*

12. That Department of State-published remarks entitled "Remarks with Kazakh Foreign Minister Saudabayev after their Meeting", dated 1 December 2010, exist and that Secretary Clinton made these statements. Admissible for non-hearsay purpose as public statements made by government officials that provide circumstantial evidence of minimized damage cause by the alleged Wikileaks disclosures. *Id.*

13. William Leonard, Director of Information Security Oversight Office of the National Archive, statements, dated 22 March 2007 given at the 2007 House Committee on Homeland Security Hearings.

14. Damage Assessments exist. *See* AE 472.

15. The Office of National Counterintelligence Executive, the Information Review Task Force, and the Department of States created or compiled their respective damage assessments on the noted dates. *Id.*

16. The Department of State damage assessment is the most current version and is a draft. *Id.*

B. For pre-sentencing proceedings, the Court will take judicial notice, conditional on the following:

1. Court will take judicial notice of the findings in Section 2 of PL 111-258 to the degree they are relevant. Such judicial notice would be the adjudicative fact that Congress made the findings (that Congress believed over-classification was a potential issue and passed this legislation – which contains not just findings but specific statutory initiatives – to address that issue), not that the findings by Congress are adjudicative fact. Thus, subject to a demonstration of relevance, the Court will take judicial notice of the existence of PL 111-258, to include the Congressional finding in Section 2, the date of introduction of H.R. 255 and the date the law was enacted. The Court will not take judicial notice of the truth of the matter asserted in PL 111-258 as adjudicative facts. AE 481.

2. The 22 March 2007 testimony of Mr. Leonard is admissible under MRE 803(8)(A), if relevant. *Id.* The key assertion cited by the Defense, that trained government classifiers only made “clearly” correct classification decisions 64 percent of the time was based on an official audit. (“In an audit of agency classification activity conducted by my office approximately one year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it right only 64 percent of the time in making determinations as to the appropriateness of classification.”).

3. That a UPI News Track news story entitled “Clinton on Leaked Documents: So What?”, dated 4 December 2010, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *See* AE 356; AE 316.

4. That a New York Times news story entitled “From WikiLemons, Clinton Tries to make Lemonade”, dated 4 December 2010, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *Id.*

5. That a CNN news story entitled “Clinton: WikiLeaks Cables Show Diplomacy at Work”, dated 4 December 2011, exists. In this instance, judicial notice is conditional on a relaxation of the rules. *Id.*

6. That an interview described on MSNBC entitled “Biden on Start, WikiLeaks” exists. In this instance, judicial notice is conditional on the defense providing the Court with the date of this interview. *Id.*

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,


Fort Myer, VA 22211

) DEFENSE CLARIFICATION  
) OF COLLOQUY FOR  
) STIPULATIONS OF EXPECTED  
) TESTIMONY (PROSECUTION  
) EXHIBITS 180 & 181)  
) ON 1 JULY 2013

) DATED: 1 JULY 2013

1. On 1 July 2013 this Court completed a colloquy with PFC Manning with respect to Prosecution Exhibits 180 and 181, which are stipulations of expected testimony for OGA Witnesses.
2. Both the Government and the Court referred to the witnesses by the number that corresponded with the witnesses on Appellate Exhibit 479, a Government *Grunden* filing. Specifically, the witness for Prosecution Exhibit 180 was referred to as #3, while the witness for Prosecution Exhibit 181 was referred to as #29.
3. During the colloquy the Defense indicated that the Defense has internally referred to the witnesses from Prosecution Exhibits 180 and 181 by their corresponding numbers from Appellate Exhibit 475, the Government's most recent witness list. Specifically, the witness for Prosecution Exhibit 180 was referred to as #23 by the Defense, and the witness for Prosecution Exhibit 181 was referred to as #107 by the Defense.
4. The Defense, per the Court's request, sets forth that the individual identified as #3 in AE 479 is the same individual identified as # 23 in AE 475. Moreover, the Defense sets forth that the individual identified as #29 in AE 479 is the same individual identified as # 107 in AE 475.
5. PFC Manning was aware of the facts set forth in paragraph 4 at the time the Court engaged him in the colloquy.

Respectfully Submitted

  
JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

589b  
PAGE RECORDED  
PAGE OF PAGES

I certify that I served or caused to be served a true copy of the above on MAJ Ashden  
Fein, via electronic mail, on 1 JULY 2013.

A handwritten signature in black ink, appearing to read 'Joshua J. Tooman', with a stylized flourish extending to the right.

JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

Appellate Exhibit 589

5 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 590

3 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**RULING: Government Motion  
To Qualify Mr. Daniel Lewis as an  
Expert**

**2 July 2013**

---

On 1 July 2013, the Government moved the Court to recognize Mr. Daniel Lewis as an Expert witness in Counter-Intelligence (CI) and value of U.S. government information to foreign intelligence sources. The Government established its foundation in both open and closed sessions. The Defense does not oppose Mr. Lewis as an expert in CI generally but does challenge his expertise in offensive CI and value. The Defense cross-examined Mr. Lewis regarding foundation in both open and closed sessions. The parties presented oral argument in closed session. Having received the briefs and having heard oral argument, the Court finds and rules as follows:

**Findings of Fact:**

1. Mr. Lewis has 29 years of experience in CI, including CI operations, investigations, collections, analysis, and functional services. Included in this experience is a tour as Chief of Training for the Department of Defense (DoD) Joint CI training academy (JCITA) for the military and the Defense Intelligence Agency (DIA). Mr. Lewis' experience includes working as a senior investigator at the Foreign CI Activity (FCA) which operates the most sensitive and significant espionage investigations.
2. From 2006 – 2013, Mr. Lewis was the Chief of the Counter Espionage Division at DIA. This was the DIA's most senior CI position. Mr. Lewis was the senior level subject matter expert for CI operations and investigations, supervising 50-55 CI professionals at any given time. He is the most experienced CI expert in DIA. The Counter Espionage Division retained oversight of all service CI investigations and operations with DoD and the National Security Agency (NSA), to include espionage investigations and offensive CI operations. Mr. Lewis personally briefed the Secretary and Under Secretary for Defense for Intelligence and Congress.
3. Mr. Lewis was a lead investigator in multiple CI investigations, including COL George Trofimoff and Army Sergeant (Ret) David Boone, both convicted of espionage in providing information to Russia. Mr. Lewis received the Civilian DoD CI Investigator of the year award for both cases, in 1996 and 1999, respectively.
4. CI investigations are espionage investigations where DoD has an equity. CI operations involve clandestine activities focused on individuals known to be involved in adversary, intelligence, or terrorist organizations. Mr. Lewis has experience as a case officer in espionage investigations but has never been a case agent or case agent manager for an offensive CI



operation. In his position as Chief of the Counter Espionage Division at DIA, he has over-sight of all DoD offensive CI operations.

5. Mr. Lewis has testified as a fact witness in court but has never been qualified as an expert witness in any court for any purpose.

**The Law:**

1. A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.

MRE 702.

2. An expert may base an opinion on facts or data in the case that the expert has been made aware of or has personally observed. If experts in the particular field would rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. MRE 703 in relevant part.

3. The Court is the "gatekeeper" for all expert testimony, whatever the basis. To allow expert testimony, the Court must find relevance and reliability. Among the factors a court may consider to determine whether expert testimony is admissible under MRE 702 is (1) whether a theory or technique has been tested; (2) whether it has been subjected to peer review and publication; (3) the known or potential rates of error in using a particular scientific technique and the standards controlling the techniques operation; and (4) whether the theory or technique has been generally accepted in the particular scientific field. These factors are not a "test" for reliability, rather reliability is a flexible inquiry focused on the goal of ensuring that the expert "whether basing testimony on professional studies or personal experience employs in the courtroom the same level of intellectual rigor that characterizes the practice of experts in the relevant field." *U.S. v. Sanchez*, 65 M.J. 145, 149 (C.A.A.F. 2007) citing *Kumho Tire Company, LTD v. Carmichael*, 526 U.S. 137 (1999).

4. Relevant evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice or other considerations enumerated under MRE 403.

**Conclusions of Law:**

1. Mr. Lewis' expertise comes from his 29 years of experience in CI investigations and oversight of offensive CI operations. He is an expert in all facets of CI. His testimony will be based on information gathered through offensive CI operations and systematically entered into systems employed by the Counter Espionage Division of DIA. These systems are routinely used by DIA to collect data from offensive CI operations and such data is used prepare briefings and other memoranda the Secretary and Under Secretary of Defense for Intelligence and for Congress and has been generally accepted by these entities as accurate. The data collected by these systems is reliable.

2. The Court has issued an oral classified supplement to this ruling. The Court accepts Mr. Lewis as an expert in CI. The Court does not accept Mr. Lewis as an expert in the value of U.S. government information to foreign intelligence services. This expertise is too overbroad. Mr. Lewis may testify and offer an opinion with regard to value of certain charged documents upon laying a proper foundation within the parameters of the oral classified supplement to this ruling.

3. The Court has done an analysis under MRE 403 and finds that Mr. Lewis' testimony is highly probative. The probative value of the evidence is not substantially outweighed by the danger of unfair prejudice or other MRE 403 factors. The Court will consider this evidence for its proper purpose within the parameters of this ruling and its oral classified supplement.

**Ruling:** The Government motion to qualify Mr. Lewis as an expert is **Granted in Part**.

So **Ordered** this 2<sup>nd</sup> day of July 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

RULING: Relevance and  
Non-Hearsay for Prosecution  
Motion for Judicial Notice

2 July 2013

On 16 January 2013, the Court deferred ruling on the Government motion for the Court to take judicial notice of certain adjudicative facts until the Government offered the evidence at trial to allow the Court to be fully informed when making relevance/hearsay determinations (AE 472). The Court ruled that it would grant the Government's motion for judicial notice if the Government could establish relevance and a non-hearsay or hearsay exception usage. On 28 June 2013, the Government renewed its request for the Court to take judicial notice of the following three adjudicative facts.

(1) Julian Assange was located in Iceland in February of 2010 and was working on the Icelandic Modern Media Initiative.

(2) LTC Packnett was quoted in a New York Times article, dated 18 March 2010.

(3) A New Yorker profile of Julian Assange titled "No secrets: Julian Assange's Mission for Total Transparency" exists and was dated 7 June 2010.

The Government also provided a proffer of relevance and non-hearsay or hearsay exception use (AE 587) and pin-point cites to admitted exhibits in support of its proffer (AE 587(a)).

Defense opposes and maintains its relevance objection to (1), (2), and (3) and hearsay objections to (2) and (3).

**The Law:** The Court adopts the law as stated in its 16 January 2013 ruling regarding judicial notice motions (AE 472).

#### Conclusions of Law:

1. The Court has reviewed the proffer by the Government and each of the pinpoint cites in support in PEs 81, 123, and 30 and the testimony of SA Shaver, and Mr. Lamo. The Court also notes the Defense conceded during the testimony of Mr. Chad Madaras that any searches on Intelink for "Iceland" and "wikileaks" in the Open Source Center on the computer shared by Mr. Madaras and PFC Manning were not conducted by Mr. Madaras.

2. Each of the three judicially noticeable adjudicative facts are relevant and are offered for non-hearsay purposes as set forth in the Government's proffer (AE 587).

**Ruling:** The Government motion for judicial notice of the adjudicative facts in (1) – (3) above is **Granted**.

So **Ordered** this 2nd day of July 2013.

A handwritten signature in black ink, appearing to read 'DRL', is positioned above the printed name.

DENISE R. LIND

COL, JA

Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION FOR**

**DIRECTED VERDICT:**

**CHARGE II, SPECIFICATIONS**

**4, 6, 8, 12 (18 U.S.C. §641**

**OFFENSES)**

DATED: 4 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty for Specifications 4, 6, 8, and 12 of Charge II.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

3. In Specifications 4, 6, and 8 of Charge II, the Government has charged that PFC Manning stole or knowingly converted the Combined Information Data Network Exchange Iraq database containing more than 380,000 records; the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records; the United States Southern Command database containing more than 700 records. In Specification 12 of Charge II, the Government has charged that PFC Manning stole or knowingly converted the Department of State Net-Centric Diplomacy database containing more than 250,000 records.

**A. The Government has Failed to Adduce Evidence that PFC Manning Stole or Converted the Databases in Question**

4. In this case, the Government has not alleged that the property of which it has been deprived were *copies* of the SIGACTs, detainee assessment briefs, and diplomatic cables or the *information* contained within certain databases. Rather, the Government has charged that PFC

Manning stole or converted the actual *databases* themselves. See Charge Sheet. In Specification 4, 6 and 8 of Charge II, the Government alleges that PFC Manning stole or knowingly converted the Combined Information Data Network Exchange Iraq *database* containing more than 380,000 records; the Combined Information Data Network Exchange Afghanistan *database* containing more than 90,000 records; the United States Southern Command *database* containing more than 700 records. In Specification 12 of Charge II, the Government pleads that PFC Manning stole or knowingly converted the Department of State Net-Centric Diplomacy *database* containing more than 250,000 records. *Id.*

5. For instance, Specification 12 of Charge II reads as follows:

In that Private First Class Bradley E. Manning, U.S. Army, did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010, steal, purloin, or knowingly convert to his use or the use of another, a record or thing of value of the United States or of a department or agency thereof, to wit: *the Department of State Net-Centric Diplomacy database* containing more than 250,000 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S. Code Section 641, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

See Charge Sheet (emphasis added). The other specifications are identical in structure. The first part of the charge mirrors the language in 18 U.S.C. §641 (“Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, ... any record, voucher, money, or thing of value of the United States or of any department or agency thereof, ...”). The sentence immediately after the expression “to wit:” explains what is alleged to have been stolen or converted—a database. That the database in question contains more than 250,000 cables is descriptive and does not alter the fact that it is the database itself that PFC Manning is alleged to have stolen or converted. In other words, PFC Manning is not charged with stealing or converting more than 250,000 cables contained within the Net Centric Diplomacy database. PFC Manning is charged with stealing or converting the database itself, which happens to contain a certain number of cables. A “database” is not in any way synonymous with the information or records contained therein. A database is a receptacle for information, much like a filing cabinet is a receptacle for paperwork. See, e.g., Stipulation of Expected Testimony of Mr. Bora (referring to CIDNE as “is a reporting and querying system”); Stipulation of Expected Testimony of Mr. Motes (noting that “[t]his database stored all detainee assessments”).

6. Notably, the Government did not charge that PFC Manning stole or converted *information* or that he stole or converted a *copy of records* contained within the database. In other words, the Government could have charged that PFC Manning stole *information*.<sup>1</sup> See e.g. *United States v.*

<sup>1</sup> The Defense would maintain, however, that information is intangible property not properly within the ambit of §641. See *United States v. Truong Dinh Hung* 629 F.2d 908, 928 (4th Cir. 1980) (“In sum, because a criminal prohibition against the unauthorized disclosure of classified information would be inconsistent with the existing pattern of criminal statutes governing the disclosure of classified information and because Congress has always refused to enact a statute like s 641 applicable to the disclosure of classified information, I would hold that s 641 cannot be interpreted to punish the unauthorized disclosure of classified information. ... Whatever the content of “thing of value” in the context of other types of government information, this phrase may not be read to include

*Jeter*, 775 F.2d 670, \*680-1 (6<sup>th</sup> Cir. 1985) (“The government charged that Jeter ‘did willfully and knowingly embezzle, steal, purloin and convert to his own use and the use of others, and without authority did sell, convey and dispose of records and things of value of the United States, the value of which is in excess of \$100.00, to wit, carbon paper and the information contained therein relating to matters occurring on October 5, 1983, before a grand jury’”). Or, the Government could have charged that PFC Manning stole a copy of government records through the use of a CD, computer time, etc. and that such records are records of the United States government. See e.g. *United States v. Fowler*, 932 F.2d 306, 309-310 (4<sup>th</sup> Cir. 1991) (“Fowler was not charged with conveying abstract information. He was charged with conveying and converting documents, which, although copies, were things of value and tangible property of the United States. True, the documents contain information, but this fact does not deprive them of their qualities as tangible property and things of value.”). See also *United States v. Hubbard*, 474 F. Supp. 64 (D.C.D.C. 1979) (“The government in response has attempted to predicate a violation of section 641 on two theories. The first is that the defendants stole the information in the documents, and the second is that the copies, allegedly made from government documents, by means of government resources, are records of the government, and thus the copies were stolen.”; court ultimately did not permit government to proceed with theory that information was stolen as it held that information was not within the scope of 18 U.S.C. §641).

7. The Government in this case did not charge that PFC Manning stole or converted “information” or “copies”; instead it charged that he stole or converted “databases.” Such a distinction is not, in any way, a semantic one: what PFC Manning is alleged to have stolen directly impacts not only the legal focus of the alleged theft or conversion (i.e. the *res* or property that was allegedly stolen), but also the valuation prong of 18 U.S.C. §641. That is, if PFC Manning is alleged to have stolen information, then the value of the information itself (and not the database) must be established. If PFC Manning is alleged to have stolen a copy of a government record, then the value of that copy must be established. Consequently, what PFC Manning is alleged to have stolen or converted is of crucial significance.

8. This proposition, while obvious, is illustrated in concrete terms using the case of *United States v. May*, 625 F.2d 186 (8<sup>th</sup> Cir. 1980). In *May*, the defendant, a former Adjutant General of the Iowa National Guard, was charged with several counts of converting *flight time* in government aircraft by directing unauthorized National Guard flights to destinations that allowed him to visit his fiancé. 625 F.2d at 188-89, 190-91. Notably, the government did not charge the defendant with converting the *entire airplane* to his own use as it was obvious that he had not stolen or converted the airplane itself. Since the property alleged to have been converted for each count was flight time, see *id.* at 190-91, and not the entire aircraft used for that flight, the

---

classified information within s 641.”); *United States v. Tobias* 836 F.2d 449 (9<sup>th</sup> Cir. 1988) (“Our circuit has adopted an even broader limitation on the scope of section 641. In *Chappell v. United States*, 270 F.2d 274 (9<sup>th</sup> Cir.1959), we held, after an extensive discussion of the legislative history, that section 641 should not be read to apply to intangible goods. This interpretation has the advantage of avoiding the first amendment problems which might be caused by applying the terms of section 641 to intangible goods-like classified information. Thus, ... we ... construe section 641 as being generally inapplicable to classified information.”). Since the Government has not alleged that PFC Manning stole or converted information, there is no need to brief this issue further. If this becomes a live issue, however, the Defense requests the opportunity to brief the question of whether information is properly within the scope of 18 U.S.C. §641.

Government sought to prove value by introducing the “cost per hour of operation for each airplane, which included the salaries of the pilots and the mechanics who serviced the planes.” *Id.* at 191. The Government did not offer evidence of the cost of purchasing and the annual cost of maintaining the entire aircraft. Rather, the Government offered evidence to prove that the value of the intangible property converted exceeded the statutory amount, as section 641 requires. Thus, *May* illustrates that stealing “an airplane” and stealing “flight time” are two very different things. First, it is clear that the accused did not steal or convert the airplane since the airplane was still available for use to the United States government. Second, given that the government in that case charged that the accused converted flight time, it was the value of that specific flight time—and not the entire airplane—that was valued for the purposes of section 641. *See also United States v. Jordan*, 582 F.3d 1239 (11th Cir. 2009) (two defendants were charged with converting certain individuals’ criminal records from within the National Crime Information Center database, rather than with a theft of the database itself; value adduced was value of the records, not the database itself).

9. If the Government in this case intended to charge theft of the *information* itself or theft of a *copy* of a record, instead of theft of the database, such a charge must appear in the Charge Sheet. *See e.g. United States v. Jeter*, 775 F.2d 670, \*680-1 (6<sup>th</sup> Cir. 1985) (“The government charged that Jeter ‘did willfully and knowingly embezzle, steal, purloin and convert to his own use and the use of others, and without authority did sell, convey and dispose of records and things of value of the United States, the value of which is in excess of \$100.00, to wit, *carbon paper and the information contained therein* relating to matters occurring on October 5, 1983, before a grand jury.’”); *United States v. DiGilio*, 538 F.2d 972 (3<sup>rd</sup> Cir. 1976) (government charged that the defendants converted to their own use “records of the United States; that is, *photocopies of official files* of the Federal Bureau of Investigation”); *United States v. Jordan*, 582 F.3d 1239, 1246 (11th Cir. 2009) (indictment under §641 alleged that defendant’s “delivered the printouts which as property of the United States had a value in excess of \$1000”; in a separate count, indictment alleged that defendant received “a thing of value of the United States, that is, information contained in the NCIC records.”). Thus, based on the charging documents, the Government must now prove that PFC Manning stole or converted the actual databases in question.

10. To analogize the charged offense to one involving tangible property,<sup>2</sup> the Government’s current charge of stealing or converting a database containing a certain number of records would be akin to charging an accused with stealing a filing cabinet containing a certain number of documents. Here, there is no evidence to suggest that the “filing cabinet” (i.e. database) was stolen or converted. The filing cabinet has remained in the exact same place and used by the government in the exact same manner before and after the alleged theft or conversion. Indeed, the filing cabinet is still available to this day and used in the same manner as it was prior to the alleged theft or conversion. Further, there is no evidence that actual documents contained within the filing cabinet were stolen or converted. To the extent that there is an argument that something was stolen or converted, it is a copy (in this case, a digital copy rather than a photocopy) of the documents contained within the filing cabinet. Stealing or converting a digital copy of a

<sup>2</sup> Section 641 has its origins in tangible property and its substance cannot be relaxed or altered to account for any difficulty that the Government may happen to encounter in using this section to charge the theft or conversion of intangible property.



document within the filing cabinet is not, by any stretch of the imagination, the same thing as stealing the filing cabinet itself. This is readily apparent when one considers valuation. One might have a filing cabinet that costs, say, \$1000, but the value of the documents contained in the filing cabinet is only \$10.00 (the cost of the paper and ink because the information contained therein is not inherently valuable). The contents of the filing cabinet are not coextensive with the filing cabinet itself either in terms of property or value.

11. To sustain a theft conviction under Section 641, the Government has the burden of proving that PFC Manning wrongfully took "property belonging to the United States government with the intent to deprive the owner of the use and benefit temporarily or permanently." To sustain a conversion conviction under Section 641, the Government has the burden of proving "a misuse [that] seriously and substantially interfere[s] with the United States government's property rights." See Appellate Exhibit 410. The Supreme Court held in *Morissette v. United States*, 342 U.S. 246 (1952) that under 18 U.S.C. §641, "[p]robably every stealing is a conversion, but certainly not every knowing conversion is a stealing." Thus, at a minimum, the Government must prove that PFC Manning's took the databases in question in a way that seriously and substantially interfered with the government's property rights in the databases.

12. In *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (per curiam), the court explained that "[t]he cornerstone of conversion is the unauthorized exercise of control over property in such a manner that *serious interference* with ownership rights occurs." 56 F.3d at 1420 (emphasis in original). *Collins* involved a Section 641 prosecution of a technical analyst at the Defense Intelligence Agency who used the agency's classified computer system to create and maintain hundreds of documents relating to the analyst's ballroom dance activities. *Id.* at 1418. In the Section 641 prosecution, the Government alleged that the defendant converted, among other things, the agency's computer time and storage space.<sup>3</sup> *Id.* The court held that there was insufficient evidence to support the charge relating to conversion of computer time and storage because the Government did not prove that the defendant's use of the system for non-work related tasks seriously interfered with the Government's property rights in that system:

[T]he government did not provide a shred of evidence in the case at bar that [defendant] seriously interfered with the government's ownership rights in its computer system. While [defendant] concedes he typed in data and stored information on the computer regarding his personal activities, no evidence exists that such conduct prevented him or others from performing their official duties on the computer. The government did not even attempt to show that [defendant's] use of the computer prevented agency personnel from accessing the computer or storing information. Thus, [defendant's] use of the government computer in no way seriously interfered with the government's ownership rights.

*Id.* at 1421.

13. Along similar lines, the Eighth Circuit in *United States v. May*, 625 F.2d 186 (1980), reversed the defendant's Section 641 conviction because the district court failed to instruct the jury that conversion under Section 641 required a finding that the defendant's conduct seriously

<sup>3</sup> Notably, the prosecution did not allege that the defendant in that case stole or converted the *computer* itself.

violated the Government's property rights. 625 F.2d at 188. In *May*, the defendant, a former Adjutant General of the Iowa National Guard, "directed a series of unauthorized flights, using National Guard aircraft, fuel and personnel, that served his own convenience rather than that of the National Guard." *Id.* at 188-89. More specifically, the defendant directed 11 unauthorized flights that allowed him to visit his fiancé in various parts of the country. *Id.* at 189. In holding that the district court's failure to instruct the jury on the serious interference element of conversion was reversible error, the *May* Court explained that:

The touchstone of conversion is the exercise of such control over property that serious interference with the rights of the owner result, making it just that the actor pay the owner the full value of the object.

\* \* \*

The problem with the district court's instruction is that it assumes that any misuse or unauthorized use of property is a conversion.

\* \* \*

[T]he instruction misses the mark because it does not mention the requirement that the misuse constitute a serious violation of the owner's right to control the use of the property.

*Id.* at 192.

14. Similarly, the Ninth Circuit in *United States v. Kueneman* reversed the defendant's Section 641 conversion conviction because of an inadequate showing that the defendant's conduct seriously interfered with the Government's property rights. No. 94-10566, 1996 WL 473690, at \*2 (9th Cir. Aug. 20, 1996) (unpublished). In that case, the defendant was the president of a non-profit organization that participated in a Department of Housing and Urban Development's (HUD) program that leased HUD homes to non-profit organizations for \$1/year, provided that the non-profit organizations agreed to sublet these homes to homeless persons. *Id.* at \*1. The defendant's alleged conversion occurred when he allowed his daughter to live in one of the HUD homes for six weeks after quarrelling with her husband. *Id.* The Ninth Circuit determined that the Government's evidence of conversion was insufficient as a matter of law. *Id.* The court explained that "not all misuse of government property is conversion. To prove conversion, the government must show [defendant's] misuse of the HUD house was a 'serious interference with the [government's] property rights.' A 'serious interference' is one that prevents the government from making some other use of the property." *Id.* at \*1-2 (internal citations omitted). The evidence of conversion was thus held to be insufficient because "[t]he government offered no evidence that it had other contemporaneous uses for the HUD home." *Id.* at \*2.

15. Thus, it is clear that the Government must show that PFC Manning's alleged actions resulted in a substantial or serious interference with the Government's use of the databases in question in order for PFC Manning to be found guilty of knowing theft or conversion of databases under Section 641. The Government has failed to offer any such evidence since it is clear that PFC Manning did not steal or convert the databases in question.

16. The Government has not introduced any evidence that the property in question here—the various databases—were ever moved, altered, corrupted, changed or taken away from the United States government. For instance, there is no evidence that WikiLeaks has, or had, the CIDNE database, the Net-Centric Diplomacy database, or the United States Southern Command database in its possession, such that it could make use of those databases. To the extent that WikiLeaks had anything, it is the information that may have been contained within the database at a certain point in time. The databases themselves always remained intact and available exclusively to the United States government.

17. Further, the Government has adduced no evidence to show that information was actually deleted or removed from the databases, such that the Government was unable to access the databases or parts thereof. The Government has not shown, for instance, that the databases were “down” for a period of time, that PFC Manning’s actions rendered the databases inaccessible, or that information was missing from the databases. *See e.g. United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (“While [defendant] concedes he typed in data and stored information on the computer regarding his personal activities, no evidence exists that such conduct prevented him or others from performing their official duties on the computer. The government did not even attempt to show that [defendant’s] use of the computer prevented agency personnel from accessing the computer or storing information. Thus, [defendant’s] use of the government computer in no way seriously interfered with the government’s ownership rights.”).

18. The Government has also not provided any evidence that suggests that PFC Manning’s actions interfered in any way with the use and benefit of the databases in question, or that his actions seriously and substantially interfered with the government’s use of the databases. The evidence shows that the databases were used in the *exact* same way both before and after PFC Manning’s disclosure of the information contained in the databases. The testimony of the unit witnesses indicates that there was no difference in the use of the CIDNE and other databases after WikiLeaks’ release of the information. The Government has not introduced evidence that the databases containing the SIGACTS, diplomatic cables or detainee briefs were of less value to the United States government after PFC Manning’s actions. The Government has thus not adduced any evidence that PFC Manning stole or converted the databases within the meaning of 18 U.S.C. §641. *See e.g. Stipulation of Expected Testimony of Mr. Bora* (“At no time was the SIGACT information charged in this case unavailable for access on the CIDNE database. Those that accessed the SIGACT database before May of 2010 did so in the same manner after May of 2010. We continue to use the SIGACTs charged in this case in the CIDNE database. To the best of my knowledge, the United States Government has never made these databases publically available.”).

19. To once again analogize the offense to the tangible world: the filing cabinets were always in the exclusive possession of the United States government; the filing cabinets were not vandalized or destroyed; the filing cabinets were not altered in any way (much less in a way that impeded the government from using them); all the components of the filing cabinets (e.g. the brackets, the tabs, the file folders) remained intact; all the files in the filing cabinet remained where they were; the filing cabinet itself was not made unavailable for others to use. The analogy to the filing

cabinet helps concretize the idea that PFC Manning in no way, shape, or form, stole or converted the databases in question.

20. The Government obviously has not charged that PFC Manning stole or converted information contained within a database. Nor has it charged that PFC Manning stole or converted copies of digital records kept by the United States government. Instead, it has charged that he stole or converted the databases themselves. Since the Government has introduced no evidence that PFC Manning stole or converted the databases in question, he must be found not guilty of the section 641 offenses.

21. Indeed, even if the Government had charged PFC Manning with theft of *information* contained within the database (rather than theft of the database itself), the Government still has not introduced evidence that PFC Manning stole or converted the information. The Government has not introduced any evidence that it lost possession or the benefit of the information in question. The information contained in the databases in question was always available to analysts and the United States government as needed. In *United States v. Jeter*, 775 F.2d 670, (6<sup>th</sup> Cir. 1985), the accused was charged with stealing carbon paper of a grand jury indictment, along with the information itself. The accused argued that he could not be found guilty under section 641 "because the government did not lose possession of any informational property due to his activities." *Id.* at 680. The Sixth Circuit responded to this argument by noting that the Government charged Jeter with stealing, purloining or converting *or* with selling, conveying and disposing of records and things of value to the United States. The Court noted:

But the government indicted Jeter under Section 641 not by simply invoking the litany of embezzlement, stealing and/or conversion. The government charged that Jeter did willfully and knowingly embezzle, steal, purloin and convert to his own use and the use of others, *and without authority did sell, convey and dispose of records and things of value of the United States*, the value of which is in excess of \$100.00, to wit, carbon paper and the information contained therein relating to matters occurring on October 5, 1983, before a grand jury.

This second half of Jeter's Section 641—regarding unauthorized selling, conveying, and disposing of records and/or things of value to the United States government—describes a set of distinguishable activities that are alone sufficient for conviction under Section 641.

*Id.* at \*680-1 (emphasis in original). It is clear that the Sixth Circuit found the evidence sufficient to support a conviction under the "sell/convey/dispose" prong of 18 U.S.C. §641, not under the "steal/purloin/convert" prong of the section. In other words, the accused conveyed records and things of value; he did not steal records and things of value.

22. Similarly, in *United States v. DiGilio*, 538 F.2d 972 (3<sup>rd</sup> 1976), the defendant argued that the government had not established a violation under section 641 on the basis that "at most, the government lost *exclusive possession* of the information contained within its confidential records, and that Congress never intended section 641, which is essentially a larceny statute, to protect the governmental interest in exclusive possession of its information." *Id.* at 977 (emphasis added). The Third Circuit, like the Sixth Circuit, avoided the issue of whether one

could be guilty of stealing or converting when the information in question was still in the possession of the United States government. Instead, the court noted that duplicate copies were made using U.S. government resources and that those copies were, in themselves, records within the meaning of 18 U.S.C. 641. *Id.* at 978 (“since there was an asportation of records belonging to the United States we need not in this case decide whether appropriation of information alone falls within section 641”). See also *United States v. Morison*, 844 F.2d 1057, 1077 (4<sup>th</sup> 1988) (distinguishing between theft of original information versus theft of copies: “Those cases involved copying. The defendant’s possession in both cases was not disturbed. This case does not involve copying; this case involves the actual theft and deprivation of the government of its own tangible property.”). These cases all suggest that an accused cannot be found guilty under the “steal, purloin or convert” portion of section 641 when the government’s possession of the property or information in question was not otherwise disturbed.

23. The aforementioned discussion of information, however, is of no consequence given the current charges that PFC Manning stole or converted certain databases (not the information contained therein). Since the Government has not introduced any evidence that PFC Manning stole or converted the databases in question, the Defense requests that this Court enter a finding of not guilty under R.C.M. 917.

**B. The Government Is Not Permitted to Amend the Charge Sheet To Now Allege that PFC Manning Stole “Information” or “Copies of Records”**

24. To the extent that the Government will now argue that it intended to charge with PFC Manning with knowing theft or conversion of *information* contained within the databases or theft of *copies* of government records (rather than charging PFC Manning with theft or knowing conversion of the databases themselves), the Defense submits that the Government is not permitted to do this, as it is outside the scope of the Charge Sheet. Should this Court consider allowing the Government to do so, the Defense requests an opportunity to further brief this issue and requests oral argument.

25. That the Government intended to charge and prove that PFC Manning stole the *databases* and not information is apparent by looking at the evidence that the Government has introduced on valuation. The Government’s witnesses all discussed in detail in their stipulations of expected testimony how much it costs to establish and maintain the relevant *databases* and associated infrastructure in various years. This clearly shows that the Government meant to charge theft of the databases—and not the information—and accordingly should be required to prove the charges in the manner charged. See also Appellate Exhibit 58 (in unreasonable multiplication of charges motion, Government emphasizing that “the 18 U.S.C. §641 offenses are aimed at the theft of United States Government-owned *databases*.”) (emphasis added).

26. Any change to the charge sheet would be a major amendment which is not permitted over the accused’s objection. See R.C.M. 603(d) (major changes “may not be made over the objection of the accused unless the charge or specification affected is preferred anew.”). Major changes “add a party, offense, or substantial matter not fairly included in those previously preferred, or which are likely to mislead the accused as to the offenses charged. R.C.M. 603(b). Only changes where “no substantial right of the accused is prejudiced” are permitted. *Id.* It

seems to be fairly obvious that the words “database”, “information” and “copy” mean different things and would have different values for the purposes of the valuation prong of 18 U.S.C. §641. Accordingly, any change as to what PFC Manning would now have to defend against would seriously prejudice his defense.<sup>4</sup>

27. In *United States v. Marshall*, No. 08-0779 (C.A.A.F. 2009), C.A.A.F. held that:

A variance that is ‘material’ is one that, for instance, substantially changes the nature of the offense, increases the seriousness of the offense, or increases the punishment of the offense.” *Finch*, 64 M.J. at 121 (citing *United States v. Teffeau*, 58 M.J. 62, 66 (C.A.A.F. 2003)). A variance can prejudice an appellant by (1) putting “him at risk of another prosecution for the same conduct,” (2) misleading him “to the extent that he has been unable adequately to prepare for trial,” or (3) denying him “the opportunity to defend against the charge.

*Id.* at 5 (available online at: <http://www.armfor.uscourts.gov/newcaaf/opinions/2008SepTerm/08-0779.pdf>).

28. In *Marshall*, the accused was charged with escaping from the custody of one, CPT Kreitman. The evidence adduced by the government at trial showed instead that the accused escaped from the custody of SSG Fleming. At the closing of the government’s case, the defense moved under R.C.M. 917 for a directed verdict, arguing that there was absolutely no testimony regarding the accused escaping from CPT Kreitman’s custody. The military judge denied the motion and convicted the accused by exceptions and substitutions of escaping from the custody of SSG Fleming.

29. C.A.A.F. held that the military judge permitting a variance in these circumstances amounted to error and that the finding of guilty needed to be set aside. C.A.A.F. elaborated:

On the facts in this case, we are convinced the substitution was material. The military judge convicted Appellant by exceptions and substitutions of an offense that was substantially different from that described in the specification upon which he was arraigned. See *Teffeau*, 58 M.J. at 67.

Although the nature of the offense remained the same – escape from custody -- by substituting SSG Fleming for CPT Kreitman as the custodian from whom Appellant escaped, the military judge changed the identity of the offense against which the accused had to defend. This denied him the “opportunity to defend against the charge.”

---

<sup>4</sup> To give just one example, had the Defense expected to have to defend against a charge that PFC Manning stole or converted information or stole or converted a copy of records, the Defense would have hired an expert on valuation. Since the Government instead charged PFC Manning with stealing a database, the Defense did not hire an expert because it knew that it could, through the Government’s own witnesses, rebut any allegation that PFC Manning stole or converted the databases.

Having found the variance to be material, we must test for prejudice. Appellant argues that the military judge's findings by exceptions and substitutions "gave the appellant no chance to defend himself against this new charge." The Government argues that there is no prejudice, because regardless of whose custody he escaped from, there was only one event, Appellant knew the nature of the offense, and was able to defend against it. We disagree. Appellant was charged with escaping from CPT Kreitman's custody; the Government presented no evidence that he was in the captain's custody, but attempted to prove that SSG Fleming was acting as CPT Kreitman's agent; the military judge found Appellant guilty by exceptions and substitutions of escaping from SSG Fleming's custody. Had he known that he would be called upon to refute an agency theory or to defend against a charge that he escaped from SSG Fleming, Appellant is unlikely to have focused his defense and his closing argument on the lack of evidence that CPT Kreitman placed him in custody or that he escaped from the custody of CPT Kreitman. "Fundamental due process demands that an accused be afforded the opportunity to defend against a charge before a conviction on the basis of that charge can be sustained." *Teffeau*, 58 M.J. at 67; accord *Dunn v. United States*, 442 U.S. 100, 106-07 (1979). Under these circumstances, we do not believe that Appellant could have anticipated being forced to defend against the charge of which he was ultimately convicted. Accordingly, we find the material variance prejudiced Appellant such that the military judge's finding by exceptions and substitutions cannot stand.

*Id.* at 7.

30. Similarly, in the instant case, changing the charge from stealing a "database" to stealing "information" or "copies of records" is a fundamental change which alters the very substance and identity of the offense as well as the accused's opportunity to defend against the charge. Just as C.A.A.F. found that escaping from the custody of CPT Kreitman was a different offense than escaping from the custody of SSG Fleming, so too is stealing or converting a "database" a different offense than stealing or converting "information" or "copies of records." The fact that all involve some form of "stealing or converting" is irrelevant and does not support the granting of a variance. In *Marshall*, C.A.A.F. outright rejected the government's argument to a similar effect:

The Government also argues that it is immaterial from whom Appellant escaped, because the escape was wrongful in any event. The fact that two alternative theories of a case may both involve criminal conduct does not relieve the government of its due process obligations of notice to the accused and proof beyond a reasonable doubt of the offense alleged. See *United States v. Ellsey*, 16 C.M.A. 455, 458-59, 37 C.M.R. 75, 78-79 (1966).

*Id.* at 9, note 3. See also *United States v. Longmire*, 39 M.J. 536, 540 (A.C.M.R. 1994) (noting that a proposed variance which substituted the violation of an order issued by one commander for the violation of an order issued by another commander "changed the essential character of the original charge" and was therefore not permissible).



31. Similarly, in *United States v. Wilkins*, 1973 WL 14267 (A.C.M.R. 1972), the accused was charged with theft of United States currency of a value of \$75.00. At trial, the government introduced proof that the accused stole a wallet, but did not specifically introduce proof of the contents of the wallet, if any. The court stated:

It appears from the briefs of both the appellant and the government that in the offense of robbery, it is necessary only to establish that something of value was taken and the kind (identity) of property taken is of no import. Thus, we are asked to make the findings conform to the proof irrespective of the pleadings. In so doing, we would find that the appellant did not, as alleged, rob Specialist Belgodere of \$75.00 in US currency, but of a wallet of some value. In our opinion such findings would so change the identity of the offense charged as to result in a fatal variance between the findings and the allegations. Accordingly, the Court must conclude that the evidence is insufficient to support the findings of guilty of Specification 2 of Charge II.

*Id.* at 639. Clearly, as the court held in *Wilkins*, the identity of the *res* that is alleged to have been stolen is critical. One cannot, after the evidence shows that what was stolen was different than what was alleged to have been stolen, change the charge sheet to have the two match up. This is, in the words of the court in *Wilkins*, a “fatal variance” that would “change the identity of the offense charged.” *Id.*

32. Accordingly, the Government is not able at this late date to change the Charge Sheet to reflect what it perhaps *should* have charged PFC Manning with. This Court, in other words, cannot make the Charge Sheet fit the evidence. And any request by the Government to do so must be denied. *See Longmire* at 539 (“The fact that the amendment was proffered by the trial counsel after the trial defense counsel had served the defense’s motion to dismiss the original specification on him, suggests that the trial counsel believed the motion had merit.”).

**C. The Government Has Failed to Adduce Any Evidence of the Value of Copies or of Information**

33. As argued, the Defense maintains that the Government charged PFC Manning with stealing “databases.” It now cannot argue that PFC Manning should be guilty of §641 offenses because its proof shows that PFC Manning stole “information” or “copies of records.” However, even if this Court were to consider an amendment to the charge sheet—which the Defense opposes—the Government still has not adduced competent evidence of valuation under §641.<sup>5</sup>

34. As a preliminary matter, the Government absolutely cannot be permitted to “mix and match” its theories and offenses. For instance, the Government cannot introduce evidence of valuation of, say, the creation of a database and then argue that PFC Manning stole or converted copies of

---

<sup>5</sup> The Defense makes this argument here simply for the sake of rebutting any potential argument that the Government will advance in response to this motion. In reality, this entire discussion of valuation is superfluous since it is clear that the Government has not established that PFC Manning stole or converted the CIDNE, Net-Centric Diplomacy and SOUTHCOM databases.



records or information in the database. Rather, if the Government introduces valuation evidence related to the creation of a database, it must prove that PFC Manning stole or converted the database itself, not information contained within the database or copies of records in the database. Conversely, if the Government argues that PFC Manning stole copies of records or information contained within the database, it must value the copies of records or information within the database. At bottom, the Government cannot be permitted to prove that PFC Manning stole copies of records or information for the purposes of establishing the "steal, purloin or convert" prong of section 641, and then prove the value of the database itself for the purposes of the valuation prong.

35. Again, to use the filing cabinet analogy, the Government cannot be permitted to argue that PFC Manning stole information or copies of records from the filing cabinet, and then rely on the value of the filing cabinet itself to establish the value of the information or copies of the records. As indicated above, one might have a filing cabinet that costs \$1000, but that does not mean that the contents of the filing cabinet are worth \$1000. They could be worth \$1, or they could be worth \$10,000. The valuation of a filing cabinet does not speak at all to the valuation of the contents contained therein. See *United States v. Wilkins*, 1973 WL 14267, \*639 (ACMR 1972) (evidence of theft of wallet did not establish that the wallet's contents were \$75.00 as charged; a variance was not permitted since this would change the "nature of the offense charged").

36. If the Court permits the Government to proceed with a charge that PFC Manning stole information or copies of records (which the Defense submits it cannot for the reasons outlined above) the Government has still not introduced even a shred of evidence as to the value of the information or copies of the records.

37. Courts have been stringent on the proof required to establish valuation for the purposes of 18 U.S.C. §641. In *United States v. Wilson*, 284 F.2d 407 (4th Cir. 1960), the Fourth Circuit stated:

A fact which distinguishes a violation punishable by imprisonment for not more than one year from a violation punishable by imprisonment for ten years cannot be permitted to rest upon conjecture or surmise. In order to sustain the imposition of the higher penalty, it was as incumbent upon the Government to prove a value in excess of \$100.00 as it was to prove the identity of the defendant as the perpetrator of the crime, or the ownership of the property.

See also *United States v. Thweatt*, 140 U.S.App.D.C. 120, 433 F.2d 1226 (1970) ("When there is a possibility of convicting the defendant of either grand or petit larceny offenses which carry significantly different penalties and which are distinguished solely by the value of the property taken it is essential that the government introduce evidence of that value in order to give the jury a firm basis upon which it can render a verdict.").

38. The leading case for this proposition is *United States v. Wilson*, 284 F.2d 407 (4th Cir. 1960). In *Wilson*, the defendant was charged with the theft of 72 rifles at a time when Section 641 only required the property to have value in excess of \$100 for a felony conviction. *Id.* at 408. Furthermore, the indictment alleged that the value of the 72 rifles was \$7,500. *Id.* at 407. The Government, however, offered no evidence at trial on the value of the rifles, but the jury still

found the defendant guilty on the felony charge. *Id.* at 408. To reach the conclusion that the rifles had value in excess of \$100, the jury only needed to infer that each rifle had a value of at least \$139. See *DiGilio*, 538 F.2d at 980-81 (discussing *Wilson*). The Fourth Circuit vacated the defendant's 7 1/2-year sentence because no evidence of the value of the rifles was offered. *Wilson*, 284 F.2d at 408. The *Wilson* Court explained its rationale as follows:

The Government . . . failed to produce any evidence whatsoever as to the value of the stolen weapons. We are asked to take judicial notice that 72 rifles are worth more than \$100.00, but we cannot on the basis of anything in the testimony form a judgment as to value for the purpose of supporting the greater penalty. Nor, in the absence of any proof of value, could the jury be permitted to speculate on this point merely from the appearance of the articles. A fact which distinguishes a violation punishable by imprisonment for not more than one year from a violation punishable by imprisonment for ten years cannot be permitted to rest upon conjecture or surmise. In order to sustain the imposition of the higher penalty, it was as incumbent upon the Government to prove a value in excess of \$100.00 as it was to prove the identity of the defendant as the perpetrator of the crime, or the ownership of the property.

*Id.*

39. Similarly, in *United States v. Horning*, 409 F.2d 424 (4th Cir. 1969), the defendant was convicted under Section 641 of stealing several tools from a military base's tool shed. 409 F.2d at 425. The only competent evidence as to the value of the tools offered at trial was the testimony of the pawn broker who lent the defendant \$50 for a portion of the stolen tools. *Id.* at 426. The Government emphasized that value of the tools in excess of \$100 could be inferred from "the 'common knowledge' that pawnbrokers do not lend the full value of pledged goods." *Id.* The *Horning* Court found this evidence insufficient to sustain the felony sentence imposed and remanded for resentencing. *Id.* at 426-27. The court explained: "[W]e think the inference the Government would draw from the stipulated testimony too speculative to establish in a criminal proceeding the value of the stolen property. Certainly no sufficient foundation was provided to enable the jury to find beyond a reasonable doubt this essential element of the offense charged." *Id.* at 426.

40. Additionally, in *DiGilio*, the Government established that the defendant purchased the stolen FBI files from a codefendant on 25-35 occasions and paid more than \$1,000 for the documents in the aggregate. 538 F.2d at 979-80. The Government contended that "because in the aggregate *DiGilio* paid over \$1,000, the jury could infer that at least one of the thefts was of records having a market value of over \$100." *Id.* at 980.<sup>6</sup> The *DiGilio* Court disagreed, concluding that:

[T]here was insufficient evidence from which the jury could infer that any of the several thefts that the [G]overnment proved was of a record having value in

<sup>6</sup> *DiGilio* was decided prior to 2004, when Section 641 was amended to permit aggregation of the value from all of the counts for which the defendant is convicted. See Identity Theft Penalty Enhancement Act, Pub. L. No. 108-275, § 4, 118 Stat. 831, 833 (2004). Thus, the issue in *DiGilio* was whether there was sufficient evidence to conclude that any one of the 25-35 purchases established value in excess of \$100. See 538 F.2d at 979-80.

excess of \$100. We do not approve the [trial] court's charge that the jury could determine the cost of gathering and producing the information or the market value in a thieves' market 'on the basis of (its) common knowledge and experience, and the reasonable inferences to be drawn from the evidence.' No reasonable inferences of market value of property involved in any particular theft could be drawn from the evidence. Permitting juror speculation as to value in the absence of evidence was, for the reasons set forth in *United States v. Wilson* and the cases which have followed it, error.

*Id.* at 981 (quoting trial court).

41. As discussed, to the extent that the Government has introduced evidence of valuation pertaining to the databases in question, such evidence is irrelevant because it is clear from the Government's evidence that PFC Manning did not steal the database (or, to use the tangible analogy, he did not steal the filing cabinet). Even if the Government sought to rely on the theft of copies of records or information, it has not produced any evidence as to the value of the copies or the value of the information.

Valuation of "Copies" of Allegedly Stolen or Converted Records

42. In addition to the market valuation method, Section 641 authorizes "cost price" as a method of proving value. See 18 U.S.C. § 641. Under this method, the cost of producing, compiling or using the item allegedly stolen or converted can be introduced to show that the item has value in excess of the statutory amount. In all prosecutions utilizing the cost price valuation method, the relevant cost is the cost of the property actually embezzled, stolen, purloined or converted—in this case, digital copies of records contained within certain databases.

43. In *United States v. DiGilio*, 538 F.2d 972 (3<sup>rd</sup> Cir. 1976), for instance, the court held that the "a duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen." *Id.* at 977. In terms of valuing this duplicate copy, the court held:

It is not necessary to accept the government's thesis in its entirety to hold that in this case a § 641 violation was established. This case does not involve memorization of information contained in government records, or even copying by thieves by means of their own equipment. Irene Klimansky availed herself of several government resources in copying DiGilio's files, namely, government time, government equipment and government supplies. That she was not specifically authorized to make these copies does not alter their character as records of the government.

*Id.*

44. Similarly, in *United States v. Zettl*, 889 F.2d 51 (4<sup>th</sup> Cir. 1989), the defendant was charged with violating Section 641 by conveying Navy documents without authority. 889 F.2d at 52. The Government indicated that it intended to prove that the documents had a value in excess of the statutory amount by showing the "'cost price' of photocopying, transportation, and the other

actual costs of the documents Zettl allegedly conveyed without authority.” *Id.* at 54. Like the Government’s case in *Fowler*, its case in *Zettl* did not rely on the costs of creating or maintaining the place where the Navy documents were kept. See also *United States v. Hubbard*, 474 F. Supp. 64 (D.C.D.C. 1979) (court allowed prosecution to proceed on theory that “the copies, allegedly made from government documents, by means of government resources, are records of the government, and thus the copies were stolen). Likewise, in prosecuting the former adjutant general in *May*, the government proved value of the property converted – flight time in government aircraft – not by offering evidence as to the value of the entire aircraft, but rather by showing the “cost per hour of operation for each airplane, which included the salaries of the pilots and the mechanics who serviced the planes.” 625 F.2d at 191.

45. All these cases illustrate the common sense proposition that if the allegedly stolen or converted property is a copy of a record, then it is the value of the copy that must be established (e.g. the cost of the CD, the time spent copying, the use of government servers etc.). The Government has introduced no evidence of the value of the copies allegedly stolen or converted in this case.

#### Valuation of “Information” of Allegedly Stolen or Converted Records

46. If the Government instead were to rely on a theory that PFC Manning stole “information” (a charge which is outside the Charge Sheet), it still has not introduced competent evidence of the value of the information allegedly stolen or converted. The most common method used to prove value of stolen or converted property under Section 641 is proof of market value of some kind. In this context, market value has been defined as “the price at which the minds of a willing buyer and a willing seller would meet.” *DiGilio*, 538 F.2d at 979. Additionally, as Section 641 punishes the embezzlement, theft, or conversion of government property, the market value of the property can be proven by reference to the “thieves’ market” for that property: “[T]he value measure contemplated by [Section] 641 is [not] restricted to an open market price ‘between honest, competent and disinterested men’. We apply to the statute what we feel is its obvious, and certainly its practical, meaning, namely, the amount the goods may bring to the thief.” *Churder v. United States*, 387 F.2d 825, 833 (8th Cir. 1968) (Blackmun, J.). Several other circuits have also approved of the thieves’ market valuation method. See, e.g., *Sargent*, 504 F.3d at 771; *United States v. Oberhardt*, 887 F.2d 790, 792-93 (7th Cir. 1989); *Jeter*, 775 F.2d at 680; *United States v. Gordon*, 638 F.2d 886, 889 (5th Cir. 1981); *DiGilio*, 538 F.2d at 979; see also *Morison*, 604 F.Supp. 655, 664-65 (D. Md. 1985).

47. Mere proof of the existence of a particular market will not be sufficient to establish that the specific property stolen or converted has value in excess of the statutory amount. See *DiGilio*, 538 F.2d at 979. In *DiGilio*, for example, the defendants were charged with stealing copies of information from FBI files. *Id.* at 976. The Third Circuit concluded that there was sufficient evidence of the existence of a thieves’ market for the converted documents. *Id.* at 979 (“There was some testimony that these documents were being peddled around town, and that others besides *DiGilio* had been approached about purchasing them. There would appear to be sufficient evidence to sustain a finding that a thieves’ market for the stolen records existed.”). Nevertheless, the *DiGilio* Court determined that “evidence showing only the existence of that market is insufficient on the question of value for felony sentences under [Section] 641.” *Id.*

The Government in *DiGilio* failed to establish the value of the stolen records on the thieves' market and the court accordingly vacated the felony sentences of the defendants and remanded for misdemeanor sentencing. *Id.* at 981, 989; *see also Sargent*, 504 F.3d at 770-71 (reversing judgment of conviction on the felony Section 641 counts because the government failed to prove value in excess of \$1,000, including a failure to show that the property had any "thieves' value" under the market valuation method).

48. Thus, in order to utilize the market value method of valuation, the Government is required to prove the existence of a particular market and that the property allegedly stolen or converted had a value in excess of the statutory amount at the time of the alleged offense. The Government has introduced no credible evidence to this effect.

49. The Government's proffered "expert," Mr. Lewis, candidly admitted that he did not consider himself to be an expert in valuation; had never valued information before; had not even seen the charged documents until last week; had spent only a few hours "researching" in preparation for his testimony; and until last week, did not even understand why he would be testifying. Despite all this, Mr. Lewis offered his opinions on the value of diplomatic cables, SIGACTS, detainee assessments briefs and the Global Address List. He has no particular or specialized knowledge of any of these categories of documents—he is simply familiar with the fact that there is a market for classified information generally.

50. Mr. Lewis' experience with the thieves' market is from the standpoint of a double-agent American seller who is purporting to sell classified information to a buyer on an artificially-created thieves' market.<sup>7</sup> Mr. Lewis admitted that part of the amount of money that a buyer would pay for classified information is for the "relationship" that the buyer is fostering with the seller. He could not apportion how much of that money is for the information and how much is for the relationship itself.

51. Mr. Lewis' "methodology" for valuing information was not reliable, neutral or trustworthy. He essentially testified that he would do a keyword search in the charged documents for certain types of information that had been sold in the past; this would then tell him that the information in question here had similar value. Although he could have, Mr. Lewis did not actually go back to information on prior sales to compare the actual content of the information to ensure its similarity and account for any of a myriad of factors which would alter its value (e.g. open source reporting, the passage of time, etc.). Nor did Mr. Lewis take into account transactions that had not ripened into sales of information. In other words, Mr. Lewis' "valuation" was completely devoid of any context, verification, or any other hallmarks of an expert opinion. Accordingly, the Government has not introduced any evidence which, together with all reasonable inferences could establish that any information in this case had a value of over \$1000.

## CONCLUSION

---

<sup>7</sup> The Defense submits that the relevant thieves' market is one where the seller is an actual thief, and not a double-agent masquerading as a thief who is selling, in part, a continuing relationship with a buyer.

52. For the reasons detailed herein, the Defense requests this Court enter a finding of not guilty under R.C.M. 917 for Specification 4, 6, 8, and 12 of Charge II.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION FOR  
DIRECTED VERDICT:  
ARTICLE 104**

DATED: 4 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty as to the Specification of Charge I.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

3. In the Court's ruling on the Defense motion to dismiss the Article 104 offense for failure to state an office, the Court indicated:

If, at trial, the Government does not prove the accused knew that by giving intelligence by indirect means, he actually knew he was giving intelligence to the enemy, the Court will entertain appropriate motions. Appellate Exhibit 81.

The Government has failed to adduce evidence which, together with all reasonable inferences and applicable presumptions, shows that PFC Manning had "actual knowledge" that by giving information to WikiLeaks, he was giving information to an enemy of the United States. Accordingly, the Defense requests that the Court grant this R.C.M. 917 motion for Charge I.

4. According to the Court's instructions:

"Knowingly" requires actual knowledge by the accused that by giving the intelligence to the 3rd party or intermediary or in some other indirect way, that he was actually giving intelligence to the enemy through this indirect means. This offense requires that the accused had a general evil intent in that the accused had to know he was dealing, directly or indirectly, with an enemy of the United States. "Knowingly" means to act voluntarily or deliberately. A person cannot violate Article 104 by committing an act inadvertently, accidentally, or negligently that has the effect of aiding the enemy.

The Government's evidence fails to show in any way that by giving information to WikiLeaks, PFC Manning had *actual* knowledge that he was giving information to the enemy.

5. The Government has introduced evidence that in his training, PFC Manning was told that the enemy uses the internet generally. The Government has not proffered any evidence, however, which shows that in his training, PFC Manning was told that a particular enemy looks at or uses the WikiLeaks website. In fact, Mr. Moul, who trained PFC Manning, testified that he had *never* heard of WikiLeaks prior to PFC Manning's arrest in this case. See Testimony of Mr. Moul. CPT Fulton testified that the only types of websites that intelligence analysts were warned about were social networking sites such as Facebook. See Testimony of CPT Fulton. None of the evidence elicited by the Government regarding PFC Manning's training, construed in the light most favorable to the Government, shows that PFC Manning had the *actual knowledge* that is required under Article 104. Similarly, the Government has introduced no evidence to suggest that PFC Manning was somehow independently aware that the enemy uses WikiLeaks. Mr. Johnson testified that his forensic investigation of PFC Manning's computer revealed no searches for the enemy, anything related to terrorism, or anything remotely anti-American. See Testimony of Mr. Johnson.

6. The Government also attempts to show that PFC Manning had actual knowledge that the enemy uses WikiLeaks by evidence and testimony related to the Army Counter-Intelligence Center (ACIC) report charged in Specification 15 of Charge II. The Government has adduced forensic evidence that PFC Manning's computer accessed the report multiple times between December of 2009 and April of 2010. The Government seeks to use the ACIC report to show that PFC Manning had actual knowledge that the enemy uses WikiLeaks and therefore, that by giving information to WikiLeaks, PFC Manning was giving information to the enemy. The Government's evidence, taken in the light most favorable to the Government cannot support a finding that PFC Manning had actual knowledge that the enemy uses WikiLeaks.

7. First, the title of the report is "Wikileaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" The question mark obviously denotes that the question is something that the U.S. government does not have an answer to. If the government had actual knowledge that the enemy uses WikiLeaks, then the title of the report would be "Wikileaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups." without a question mark. If the U.S. government does not have actual knowledge of the enemy's use of the WikiLeaks website, then neither can PFC Manning.



8. Second, the Government has introduced evidence that the report says that "In addition, it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the Wikileaks.org Web site." See ACIC Report. The very nature of a presumption is that a person does not know whether something is true or not true. The fact that PFC Manning should have presumed something may go to whether he was negligent or reckless, but it does not go to whether he had actual knowledge under Article 104.

9. Third, the Government's focus on one small section ignores the plain limitation laid out in the ACIC document under the section entitled "Intelligence Gaps." In the ACIC document, the author readily admits that an intelligence gap is "Will the Wikileaks.org Web site be used by FISS, foreign military services, foreign insurgents, or terrorist groups to collect sensitive or classified US army information posted to the Wikileaks.org Web site?" Ms. Glenn confirmed that an intelligence gap is something that is not able to be confirmed, or it would not be listed in that section. See Testimony of Ms. Glenn. Additionally, multiple unit witnesses testified during the Government's case that an intelligence gap is something that we *do not have actual knowledge of*. If one had actual knowledge of something, it would not be called an intelligence gap.

10. The Government also introduced testimony from Mr. Lamo where the Government sought to introduce various of PFC Manning's admissions. During cross-examination of this Government witness, the Defense elicited (and the Government did not dispute) evidence as to PFC Manning's state of mind. At one point, Mr. Lamo asked PFC Manning why he did not sell the information to a foreign government and "get rich off it[.]" In response, PFC Manning expressly disclaimed any intent to help any enemy of the United States:

[B]ecause it's public data . . . it belongs in the public domain . . . information should be free . . . it belongs in the public domain . . . *because another state would just take advantage of the information . . . try and get some edge . . . if it's out in the open . . . it should be a public good.*

See Prosecution Exhibit 30. PFC Manning's state of mind and professed motive for releasing the charged documents to WikiLeaks belies any argument that PFC Manning had actual knowledge that by giving information to WikiLeaks, he was giving information to the enemy. Indeed, PFC Manning refused to sell the information to another country, even though he could have financially benefitted by doing so, because he did *not* want an enemy of the United States to "take advantage of the information[.]" *Id.* The chat logs show that since PFC Manning did not intend to aid the enemy, he also did not knowingly give intelligence information to the enemy.

11. In the end, the Government's evidence indicated that PFC Manning spoke, via computer, with two witnesses about the charged offenses as he was committing them or immediately after the fact. During these times, PFC Manning never once mentioned AQ, AQAP, UBL, Adam Gadahn, or any potential enemy that has ever, at any time, been identified by the Government. Based upon the chat logs with Mr. Lamo, it is clear that PFC Manning's focus was on getting certain information to the American public in order to hopefully spark change and reform. There is, simply put, no evidence before this Court that PFC Manning ever possessed the "general evil intent" that must be shown in order to sustain a finding of guilt under Article 104. At most, the

Government has introduced evidence which might establish that PFC Manning "inadvertently, accidentally, or negligently" gave intelligence to the enemy. This is not sufficient to prove an Article 104 offense. *See United States v. Olson*, 20 C.M.R. 461, 464 (A.B.R. 1955) (Article 104 "does require a general evil intent in order to protect the innocent who may commit some act in aiding the enemy inadvertently, accidentally, or negligently."). Accordingly, the Article 104 offense must be dismissed.

#### CONCLUSION

12. In light of the foregoing, the Defense requests this Court grant the requested R.C.M. 917 motion for Charge I (the Article 104 offense).

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. E. Coombs', written over a horizontal line.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION FOR  
DIRECTED VERDICT:  
18 U.S.C. 1030 OFFENSE**

DATED: 4 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty for Specification 13 of Charge II.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

**A. The Government's Theory is Legally Deficient**

3. During the motions phase of this case, the Defense brought two separate motions to dismiss the 18 U.S.C. §1030 offenses based upon the Government's failure to state an offense. The Court ruled, in response to the first motion, that the Court would adopt the narrow view of *United States v. Nosal*, 676 F.3d 854 (9<sup>th</sup> Cir. 2012) such that the Government would not be able to bootstrap use restrictions (improper use of information) into access restrictions for the purposes of 18 U.S.C. §1030. The Government thereafter shifted its theory of criminality to focus on PFC Manning's use of an apparently unauthorized program to ground an offense under section 1030. The Court, not having the benefit of evidence on this point, did not dismiss the offenses and reiterated that the military justice system is a notice pleading jurisdiction and that the charge was sufficient to state an offense.

4. Now that the Court has had the full benefit of all the evidence on the issue of access to the NetCentric Diplomacy database, the Defense moves this Court to dismiss the charge under R.C.M. 917.

5. The Government's theory of liability is the following:

In order for a person to access or obtain a diplomatic cable on the NCD website, the person has to individually "click" or "save" the diplomatic cable after searching for the cable or navigating to the cable in some manner. As the evidence will show, the accused bypassed the ordinary method of accessing information by adding unauthorized software to his SIPRNET computer and using that software to rapidly harvest or data-mine the information. Wget was not available on the computers used by the accused or authorized as a tool to download the information. Thus, the accused violated a restriction on access to the information - he bypassed a code-based restriction - by using Wget to obtain the cables in batches.

See Appellate Exhibit 188 at p. 5.

6. The Government has introduced evidence that PFC Manning used the program Wget to download the diplomatic cables. However, PFC Manning's purported use of this allegedly unauthorized program<sup>1</sup> to download the information specified in Specification 13 of Charge II does not change and cannot change the only fact that matters in the "exceeds authorized access" inquiry: PFC Manning was authorized to access each and every piece of information he accessed. The Government has not introduced any evidence to suggest that PFC Manning was not permitted to view the cables in question. The Government has not introduced any evidence to suggest that PFC Manning was not permitted to download the cables in question. The Government simply asserts that PFC Manning was not permitted to download them using a certain program, Wget.

7. The Government has not introduced evidence that Wget in some way expanded the access that PFC Manning had, such that it gave him access to information that he otherwise would not have had access to. The Government's witness, Agent Shaver, testified that: Wget does not give a user access to information that they otherwise would not have access to; Wget would not allow a user to grab information that they would not normally be able to see; Wget would not allow the user to circumvent any sort of restrictions that the Net-Centric Diplomacy database may place on the user; and Wget would not give a user any more access than they would have normally. See Testimony of Agent Shaver. The Government has thus not introduced evidence that PFC Manning by-passed any restrictions on access that would give PFC Manning access to information that he otherwise would not have had access to. All the Government has to hang its hat on is that PFC Manning used allegedly "unauthorized software" -as defined by an AUP that the Government could not even produce—in downloading the cables. This does not come close to establishing "exceeds authorized access" within the meaning of 18 U.S.C. §1030.

8. The Government is simply incorrect in asserting that the use of an unauthorized program to download information automatically converts what would otherwise be authorized access to that information into "exceeding authorized access." Whether or not PFC Manning used Wget to download the information he had access to is irrelevant; under the language of Section 1030, as well as this Court's ruling and all legal authorities, PFC Manning could not have exceeded his

---

<sup>1</sup> The Defense contests that this program was unauthorized, *infra* at C.

authorized access because he was authorized to obtain the *information* he obtained. That is, “exceeds authorized access” is not concerned with the *manner* in which information to which one has access is downloaded; it is rather concerned with whether the accused was *authorized to obtain or alter the information* that was obtained or altered.

9. Section 1030(e)(6) defines “exceeds authorized access” as follows: “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]” 18 U.S.C. § 1030(e)(6). This definition demonstrates that the Computer Fraud and Abuse Act (CFAA) is concerned with the relationship between the accesser and the *information*: is the accesser entitled to obtain or alter the information at issue? In *United States v. Nosal*, the en banc Ninth Circuit explicitly tied the concept of “exceeds authorized access” to the defendant’s authorization to access the particular *information* at issue: “‘exceeds authorized access’ would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*).” 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (second emphasis supplied); *see also* Appellate Exhibit CXXXIX, at 7 (“*Nosal III* defines ‘exceeds authorized access’ to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files.” (emphasis in original)). Nothing in the discussion of the narrow interpretation of “exceeds authorized access” in *Nosal* gives any indication that the manner in which a person downloads information has any bearing whatsoever on whether the person is authorized to access that information.

10. In this case, the Government does not dispute that PFC Manning was entitled to access the information and has offered no proof that PFC Manning was not authorized to access the cables. Similarly, the Government does not dispute that PFC Manning was entitled to download the information and has offered no proof that PFC Manning was not authorized to download the cables. The Government’s Wget theory—that PFC Manning exceeded authorized access by using an unauthorized program to download the information—erroneously focuses on the manner in which PFC Manning downloaded the information. But the manner in which he downloaded the information is beside the point, since at all times he remained entitled to access the information in question.

11. The ridiculousness of the Government’s theory is highlighted when one really distills what the Government is saying. If PFC Manning had downloaded the cables one-by-one (or with a program like Excel which was in the baseline package for the DCGS-A machines), then PFC Manning would not be facing a ten-year prison sentence under 18 U.S.C. §1030. However, because he is alleged to have used a program not technically approved on his DCGS-A machine, he is facing a ten-year prison sentence. A decade in jail cannot turn on what programs the Army happens to put on its “authorized software” list. While the Defense concedes that releasing the diplomatic cables was a criminal offense—one for which PFC Manning has accepted responsibility—it is not, under any stretch of the imagination, a computer crime within any rational meaning of 18 U.S.C. §1030.

12. If computer crimes will now turn on whether an accused uses unauthorized hardware or software to look at or download information that they otherwise have access to, this would be an extremely dangerous (not to mention unconstitutional) application of the statute. This is particularly so considering that 18 U.S.C. §1030(2)(C) criminalizes “exceeding authorized

access” and “thereby obtain[ing] information from any protected computer.” In other words, simply “exceeding authorized access” and obtaining *any* information from a government computer would subject an accused to imprisonment. No particular type of information is required to have been accessed, nor does the information have to have been transmitted. It is simply “getting” the information by means of exceeding authorized access which is criminal. Consider what this would mean in practice if one could exceed authorized access simply by using unapproved hardware or software to view, download or print information that the accessor is otherwise entitled to view, download or print. A soldier who connected a commercial printer to a government computer (rather than a government-approved printer) would be exceeding authorized access if he printed any documents. A soldier who used an unapproved storage device (rather than a government-approved storage device) would be guilty of exceeding authorized access if he saved some documents onto it. A soldier who used the newest unapproved version of Excel to download information (rather than the government-approved version of Excel) would be guilty of exceeding authorized access. What most, and certainly those in PFC Manning’s Brigade, would consider a minor breach of information assurance protocols would now be a felony.

13. There is absolutely no legal precedent for the Government’s argument that the specific program with which information is downloaded can determine whether a person “exceeds authorized access” within the meaning of 18 U.S.C. §1030. A survey of the case law reveals that no criminal prosecutions have been maintained based on a theory in the nature of that advanced by the Government here (i.e. that the accessor was permitted to access the information, was permitted to download the information, but was not permitted to download the information using a certain program).

14. One civil case, however, made allegations very similar to those in the instant case. In *Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963 (D.N.H.), the plaintiff hospital alleged that certain doctors violated 18 U.S.C. §1030 on the basis that they downloaded information that they were otherwise entitled to access onto “extraordinarily large” unauthorized storage devices. The plaintiff pointed to the equivalent of the hospital’s Acceptable Use Policy (WDH Policy Document IM-09) to show that the use of unauthorized storage devices to download information that one had authorized access to was prohibited by 18 U.S.C. §1030. The complaint laid out the relevant provisions of the hospital’s computer policy (similar to the Army’s policy) as well as the plaintiff’s theory that the use of unauthorized hardware rendered the defendant’s access to information unauthorized:

20. Pursuant to IM-09, Attachment 1, Section D (“Electronic Information”):

4. No external hardware will be brought in and connected into the hospital information network without the approval of the Information Systems Department.

5. No software from external or unauthorized sources will be loaded on hospital computers without the approval of Information Systems. The hospital retains the right to remove any unauthorized or unlicensed

software from any hospital computers. Any person found loading or using unapproved software will be considered in breach of this policy.

...

43. Between February 1, 2010 and February 28, 2010, removable storage devices or external hardware were connected to PY001, PY002 and the HP Laptop. Late on February 28, 2010, the last day when Dr. Moore and Dr. Littell had access to the desk top computers and laptop, *extraordinarily large removable storage devices* were attached to each of PY001, PY002 and the HP Laptop.

...

72. Defendants intentionally accessed computers without authorization or exceeded authorized access, and thereby obtained information from a protected computer in that Defendants, without the prior authorization and approval of the WDH Information Systems Department and in violation of IM-09, connected removable storage devices or external hardware to PY001, PY002 and the HP laptop computer, and obtained or altered information from WDH computers owned by WDH that Defendants were not entitled to obtain or alter.

See 2010 WL 4786559 (D.N.H.). In short, the plaintiff hospital alleged that the defendant doctors exceeded their authorized access under 18 U.S.C. §1030 because they downloaded information onto “extraordinarily large” removable storages devices or external hardware that was not authorized under the governing computer policy. Notably, the plaintiff did not allege that the defendants were not permitted to access the information in question or were not permitted to download the information in question. The plaintiff simply alleged that accessing information *in this particular manner*—i.e. by downloading that information onto “extraordinarily large” removable storage devices that were not authorized—violated 18 U.S.C. §1030. Thus, the allegations in *Wentworth-Douglass* mirror those in the instant case. In neither case is it disputed that the accessor of the information had permission to access or download the information. In both cases, the issue is whether the accessor had permission to download information *in a particular manner* (i.e. through an unauthorized storage device or through an unauthorized program).

15. The court in *Wentworth-Douglass* framed the issue as follows:

Mirroring the language of the CFAA, count one of the amended complaint alleges that “Defendants intentionally accessed computers without authorization or exceeded authorized access, and thereby obtained information from a protected computer.” Amended Complaint (document no. 68) at para. 82. But, in elaborating on that claim, the hospital says: Count I [of the amended complaint] alleges the Defendants violated [18 U.S.C. § 1030(a)(2)(C)] because, without the prior authorization and approval of the WDH Information Systems Department and in violation of the IM-09, they connected *removable storage devices* or external hardware to hospital computers and obtained or altered information from WDH computers owned by WDH that *they were not entitled to obtain or alter*.

Plaintiff's Motion for Summary Judgment (document no. 81-1) at 13 (emphasis supplied).

...

With respect to Dr. Cheryl Moore and Dr. Littell, the issue presented is whether they can be liable under section 1030(a)(2)(C) for having violated the hospital's computer use policy when they allegedly connected removable storage devices to hospital computers and then downloaded and/or copied data that they were otherwise authorized to access.

*Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963, \*3 (D.N.H.). The court held that the defendants could *not* be liable under 18 U.S.C §1030 when they downloaded/copied data that they were otherwise authorized to access onto unauthorized storage devices. Accordingly, the court entered a directed verdict for the defendants.

16. The court saw the relevant inquiry as whether or not the defendants were authorized to access the "hospital's computer and the data at issue," not whether the defendants were authorized to download the information onto unauthorized storage devices. *Id.* at \*4. The plaintiff tried to characterize the hospital's computer policy prohibiting unauthorized hardware (the equivalent of the Army's AUP) as being an "access restriction" and not a use restriction. The court outright rejected this argument:

The court disagrees. Of course, the distinction between an employer-imposed "use restriction" and an "access restriction" may sometimes be difficult to discern, since both emanate from policy decisions made by the employer—decisions about who should have what degree of access to the employer's computers and stored data, and, once given such access, the varying uses to which each employee may legitimately put those computers and the data stored on them. But, simply denominating limitations as "access restrictions" does not convert what is otherwise a use policy into an access restriction. Here, the hospital's policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an "access" restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access. An employee who is given access to hospital data need not "hack" the hospital's computers or circumvent any technological access barriers in order to impermissibly copy that data onto an external storage device. The offending conduct in such a case is misuse of data the employee was authorized to access, not an unauthorized access of protected computers and data.

*Id.* So too is the case here. In fact, the *Wentworth-Douglass* court's rejection of the possibility of civil liability under section 1030 in circumstances very similar to those alleged here should sound a note of extreme caution to a criminal court. If the "unauthorized hardware/software" theory is not sufficient to ground civil liability, surely it is not sufficient to ground criminal liability. And indeed, there is *no criminal* case that has accepted the narrow view of the Computer Fraud and Abuse Act (i.e. the *Nosal* view) where a theory like the Government's



(accused had access to download, but didn't have permission to download with a particular program) has even been advanced, much less where the theory has succeeded. Thus, under the authority of *Wentworth-Douglass*, the only case to make allegations similar to those in the instant case, PFC Manning cannot be found criminally liable under 18 U.S.C. §1030 for violating the terms of the Acceptable Use Policy when he was permitted to access the information in question and was permitted to download the information in question.

17. Additional authority that a violation of a computer use policy cannot turn what is otherwise authorized access into "exceeds authorized access" is found in the recent Fourth Circuit decision in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4<sup>th</sup> Cir. 2012). In that case, the plaintiffs advanced the argument that the defendants exceeded authorized access within the meaning of 18 U.S.C. §1030 because "under WEC's [the employer's] policies they were not permitted to download confidential and proprietary information to a personal computer." *Id.* at 202. The district court held that the complaint failed to state an offense because "Appellees' alleged conduct—the violation of policies regarding the use and downloading of confidential information—did not contravene any of these [section 1030] provisions." *Id.* On appeal, the Fourth Circuit affirmed the district court's judgment:

WEC founds its CFAA claim on Miller's and Kelley's violations of its policies "prohibiting the use of any confidential information and trade secrets unless authorized" and prohibiting the "download[ing] [of] confidential and proprietary information to a personal computer." Notably, however, WEC fails to allege that Miller and Kelley accessed a computer or information on a computer without authorization. Indeed, WEC's complaint belies such a conclusion because it states that Miller "had access to WEC's intranet and computer servers" and "to numerous confidential and trade secret documents stored on these computer servers, including pricing, terms, pending projects [...] and the technical capabilities of WEC." Thus, we agree with the district court that although Miller and Kelley may have misappropriated information, they did not access a computer without authorization or exceed their authorized access.

*Id.* at 206-207.

18. The Fourth Circuit specifically held that the manner in which a defendant accessed information (in particular, by the unauthorized downloading onto a personal computer) could not ground civil liability, much less criminal liability, under 18 U.S.C. §1030. In this respect, it stated:

Nevertheless, because WEC alleges that Miller and Kelley obtained information by downloading it to a personal computer in violation of company policy, we go a step further. Although we believe that interpreting "so" as "in that manner" fails to subject an employee to liability for violating a use policy, we nonetheless decline to adopt the *Nosal* panel's interpretation of the conjunction. The interpretation is certainly plausible, but it is not "clearly warranted by the text." Indeed, Congress may have intended "so" to mean "in that manner," but it "could just as well have included 'so' as a connector or for emphasis." Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the

more obliging route. “[W]hen [a] choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.”

Here, Congress has not clearly criminalized obtaining or altering information “in a manner” that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter. And lest we appear to be needlessly splitting hairs, we maintain that the *Nosal* panel’s interpretation would indeed be a harsher approach. For example, such an interpretation would impute liability to an employee who with commendable intentions disregards his employer’s policy against download information to a personal computer so that he can work at home and make headway in meeting his employer’s goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But under the *Nosal* panel’s approach, because he obtained information “in a manner” that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be liable under the CFAA. See §1030(a)(2)(C). Believing that Congress did not clearly intend to criminalize such behavior, we decline to interpret “so” as “in that manner.”

*Id.* at 205-206. Notably, the Fourth Circuit’s passage referred to the Ninth Circuit panel’s decision on the word “so” which was ultimately overruled *en banc* in *Nosal*, 676 F.3d 854 (9<sup>th</sup> Cir. 2012). Accordingly, and in light of the *en banc* decision in *Nosal*, the reasoning of the Fourth Circuit is even more persuasive that the manner in which information is downloaded is irrelevant to the “exceeds authorized access” inquiry.

19. In short, the Government has provided no evidence that PFC Manning was not authorized to access each and every piece of information covered in Specification 13 of Charge II. It instead argues that his use of Wget to download the information specified in Specification 13 renders his otherwise authorized access to that information an excess of his authorization. Such a theory finds no support in Section 1030, its legislative history, and the rulings of this Court and so many others that have adopted the narrow interpretation of “exceeds authorized access.” Under that narrow interpretation of the phrase, the only inquiry is whether the accessor is entitled to obtain or alter the information at issue; the manner in which that information is downloaded does not provide an answer to that inquiry. Therefore, since PFC Manning was authorized to access all of the information covered in Specification 13 of Charge II, PFC Manning must be found not guilty.

**B. The Government Has Not Introduced Evidence that Using Unauthorized Software was an Access Restriction**

20. Even if one accepts that the Government’s theory is not legally deficient, the Government has still not established that installing and using unauthorized software was an *access* restriction. According to the Government, the prohibition on using unauthorized software generally (but not Wget specifically) is found in the Army’s Acceptable Use Policy (AUP). If the Army wanted to

create an access restriction, it must do so in a more clear way than burying it in a generic, multi-page, multi-topic AUP.<sup>2</sup> See *United States v. Nosal*, 676 F.3d 854, 860 (9<sup>th</sup> Cir. 2012) (“Significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.”).

21. Critically, the Government has not even presented the AUP signed by PFC Manning or anyone in his brigade. Thus, it is impossible to determine exactly what PFC Manning knew or should have known in terms of limitations on access and/or use.<sup>3</sup> Second, to state the obvious—the AUP refers to the Acceptable *Use* Policy, not the Acceptable *Access* Policy. This very fact shows that the policy focuses on *use* restrictions and not *access* restrictions. Third, the provision in the sample AUP regarding unauthorized software states, “d. I will *use* only authorized hardware and software I will not install or *use* any personally owned hardware, software, shareware, or public domain software.” The fact that the word “use” appears twice in this sentence clearly shows that this is a “use” restriction and not an “access” restriction.<sup>4</sup>

22. The Government has provided no evidence to show that the prohibition against unauthorized software was an *access* restriction. The Government has called no witness to say that PFC Manning understood (or that soldiers in general understood) that the use of unauthorized software was a limitation on computer access, rather than use, and that any exceeding of that access could result in a felony conviction. Without an understanding that the use of unauthorized software constituted an access restriction, a soldier (in this case, PFC Manning) could not have *knowingly* exceeded authorized access by installing and using such software.

23. Further, the Government has introduced no evidence to show that computer access of soldiers who used unauthorized software was suspended. The evidence elicited showed that members of the S-2 section constantly added what would be considered “unauthorized software” to their DCGS-A computers. If the adding and using of unauthorized software was an “access” restriction, then presumably these soldiers would have had their access circumscribed or suspended for exceeding their authorized access. The testimony shows otherwise. CPT Cherepko testified that if he was able to identify the individual who added unauthorized software, he would “go to that soldier and explain the reasons why it’s a bad idea.” See

---

<sup>2</sup> The Defense adheres to the position that allowing employers, including the Army, to develop contract-based access restrictions would render 18 U.S.C. §1030 constitutionally vague and/or overbroad. See *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). If the Army could simply make all use restrictions look like access restrictions (e.g. by stating “access to this computer system is conditioned upon a soldier using approved U.S. Government hardware and software”), this would criminalize a huge swath of conduct that is currently only punishable as a violation of a regulation. Moreover, to the extent that this Court believes that an AUP may contain both use and access restrictions, it needs to be clear to soldiers which one is which since an access restriction can render a soldier liable to imprisonment under 18 U.S.C. §1030, while a use restriction cannot.

<sup>3</sup> The testimony elicited by the Government established that there is a difference between “unauthorized software” (which is installed onto computers) and “executable files” (which are not installed onto the computer but only require a “double click”). Wget falls into the latter category. The Government has not provided any evidence that the AUP signed by PFC Manning even prohibited the use of executable files.

<sup>4</sup> No court that has accepted the narrow view of *Nosal* has found that an Acceptable Use Policy or the like can define access restrictions, rather than use restrictions. And for good reason. If all that is required to convert what otherwise is a use restriction into an access restriction is to change the phraseology of the provision, then employees will face criminal liability for breaches of contract that do not involve exceeding authorized access under any sensible understanding of the term.

Testimony of CPT Cherepko. Communicating that something is a “bad idea” is very different than communicating that something is an *access* restriction (i.e. that a soldier’s access to a computer is contingent upon not using unauthorized software). It is clear that the installation and use of unauthorized software was always treated as a use restriction—and, as described below, one that was not ever enforced by the brigade.

24. The Government has also failed to introduce any evidence that there were any access restrictions on the Net-Centric Diplomacy database itself. The Government has not introduced evidence, for instance, that the Net-Centric Diplomacy database prevented downloading information using a program like Wget; indeed, the evidence was to the contrary—that there were no technical access restrictions on downloading the information or on the manner of downloading the information. Mr. Wisecarver testified that there were no access restrictions on the Net-Centric Diplomacy database. *See* Testimony of Mr. Wisecarver (“But, again, understanding that NCD was a web-based type of application, so I don’t believe it was limited at all. If you had access to SIPRNET, you had that secret clearance, you were given authorization to use SIPRNET, then by default you would have access to NCD”). Mr. Wisecarver further testified that there were no individual access or authentication restrictions on the Net-Centric Diplomacy database and that a user could have multiple cables open at the same time which the user could download or print simultaneously.

25. Similarly, the Government has not introduced evidence of non-technical barriers on access, such as a banner on the Net-Centric Diplomacy database that said something to the effect of “This database must be accessed only with government-authorized hardware and software”<sup>5</sup> or “Information in this database may not be downloaded using automated tools.” The banner that did appear on the Net-Centric Diplomacy database focused on the *use* of the information; it did not speak at all to the manner of access. *See* Testimony of Mr. Wisecarver (stating that the banner did not specify any restrictions on how information was accessed, or on the manner of downloading cables; nothing in the warning indicated that a user had to ‘click, open, save’); *see also* Testimony of COL Miller (stating that the Brigade did not put out any restriction on the manner of downloading information from the SIPRNET or require that soldiers “click, open, and save” information). Accordingly, the Government has not established that anything resembling what might be considered an access restriction appeared on the Net-Centric Diplomacy database.

### **C. The Government Has Not Introduced Evidence that PFC Manning Knowingly Exceeded Authorized Access**

26. The Government has presented evidence that Wget was not on the approved list of programs for the DCGS-A computer used by PFC Manning in downloading the cables. Thus, it argues that since PFC Manning downloaded information that he was otherwise entitled to download with “unauthorized software” he thereby exceeded his authorized access within the meaning of 18 U.S.C. §1030.

---

<sup>5</sup> The Defense submits that this would not actually be an access restriction. It would be a *use* restriction, masquerading as an access restriction.

27. The Government has not proven that Wget, which is an executable file, was "unauthorized software" in the particular environment in which PFC Manning worked.<sup>6</sup> While it may not have been officially approved for use on the DCGS-A computer, whether or not something is "authorized" or "unauthorized" is determined by a lot more than a piece of paper. For instance, Mr. Weaver, the Information Assurance manager who testified as to the scope and content of Army Regulation 25-2, was asked whether soldiers were authorized to use games, movies, music and other executable files. In response, he stated "You want the regulation answer or my opinion, sir?" See Testimony of Mr. Weaver. The answer and explanation given by Mr. Weaver demonstrates that there can be a disconnect between what the rules are "on paper" and what the rules are in practice. This disconnect is bolstered by the testimony of COL Miller. COL Miller testified that technically unauthorized media could be approved for morale and welfare purposes. See Testimony of COL Miller ("Because sometimes these risks -- the reason given for it's not authorized is because there's a document that says this is not authorized and therefore it's a risk. What I always want to get to is why, not the document, but what was the logic behind that being put in that document so I can get to the root reason."). This fact further highlights the distinction between what the rules were on paper as opposed to what the rules were in practice.

28. The Defense submits that the use of executable files was permitted by the S-2 section, and therefore Wget was not unauthorized. Every unit witness called by the Government testified that there was music, movies and games on the computers in the T-SCIF (whether on the T-drive or on the individual computers themselves). See e.g. Testimony of CPT Cherepko; Testimony of Mr. Maderas; Testimony of CW2 Balonek; Testimony of Ms. Showman; Testimony of COL Miller. Further testimony of some of these witnesses established that at least some of these music, movies and games took the form of executable files which were run directly from the desktop.

29. Mr. Maderas testified that PFC Manning added mIRC-chat to his computer and the computer of others as an executable file. mIRC-chat was not a standard program on the DCGS-A machines. Mr. Maderas testified that he believed this was permitted and did not think it was a problem that the mIRC-chat executable file was added by PFC Manning rather than Mr. Millman. See Testimony of Mr. Maderas. Similarly, Ms. Showman also testified that she asked PFC Manning to put mIRC-chat on her computer and that he did. She did not believe that the adding of mIRC-chat by PFC Manning, as opposed to Mr. Millman, was a violation of the user agreement.

30. Unit witnesses testified that no soldier was, to their knowledge, ever punished for the placement or use of unauthorized software on the DCGS-A machines. See e.g. Testimony of Mr. Maderas. Testimony from CPT Cherepko confirmed that the command had actual knowledge of the use of executable files on the DCGS-A machines and did not do anything about it. CPT Cherepko confirmed that there was a command laxity with regard to the use of executable files.

---

<sup>6</sup> Both the Government and Defense elicited testimony that Wget was an executable file, meaning that the file is not a program that is "installed" onto the computer. Instead the program runs from the desktop after double-clicking or runs from a compact-disc. Executable files do not require administrative rights to run. See Testimony of CPT Cherepko ("There is no installation process. If you have it on a CD or thumb drive or on your desktop you can simply run it. There's no administrative rights required.").

See Testimony of CPT Cherepko. It is clear that soldiers in the S-2 shop were permitted to add executable files to their computers and did so on a regular basis. It is also clear that the chain of command knew about this rampant practice and did nothing about it. In short, soldiers in the T-SCIF were allowed to place executable files on their computer, despite the apparent on paper prohibition against adding "unauthorized software." In the S-2 shop, executable files were not considered "unauthorized software." Thus, in using an executable file, Wget, to download the cables, PFC Manning did not use "unauthorized" software. Instead, he used an executable file—a practice that had been sanctioned and approved of by the S-2 leadership and the chain of command.

31. If the Court nonetheless believes that, despite the practice in the S-2 shop, PFC Manning nonetheless used "unauthorized software", the Government has still failed to prove that PFC Manning *knowingly* exceeded his authorized access. If the Government's theory of exceeds authorized access is that PFC Manning used unauthorized software, then he must have *knowingly* used unauthorized software. Given the evidence elicited from all the unit witnesses as to what they believed was permitted and what they believed was not permitted, the Government has not introduced any evidence that PFC Manning *knew* he was exceeding his authorized access by using an executable file to download information that he had authorized access to.

32. For instance, CW2 Balonek testified that he did not know whether the use of executable files in the form of games, movies or music was authorized or not. He testified that he believed that games were allowed, if work was low. He further testified that the rules in garrison were different than the rules in theater ("different rules for different areas"). See Testimony of CW2 Balonek. Similarly, Mr. Maderas testified that he did not know whether the use of unauthorized software in the form of games, movies or music was prohibited. In response to the Court's question, he said that there was "silence" on whether this was authorized or not. See Testimony of Mr. Maderas. Ms. Showman testified that she believed that the S6 approved of music, movies and games on the DCGS-A computers, or at least she assumed they were authorized since the command knew about them and did nothing about it. See Testimony of Ms. Showman. It is clear that, at the very least, the rules of the game in the T-SCIF were unclear as to what was authorized and what was not. Accordingly, and against this backdrop, there is no evidence that PFC Manning knew that by using Wget, an executable file, he was exceeding authorized access.

33. Importantly, the fact that PFC Manning knew that ultimately transmitting the cables was wrong does not mean that he knew that his *use of the computer* in those circumstances was wrong. See 1996 Legislative History of 18 U.S.C. 1030 ("It is the *use of the computer* that is being proscribed, not the unauthorized possession of, access to, or control over the information itself.") (emphasis added). Section 1030 criminalizes those who "knowingly" exceed authorized access. Thus, the Government must show that PFC Manning knew that, by using an executable file to download information to which he otherwise had full access, PFC Manning was exceeding the access he was given. In light of what was permitted at the S-2 shop in terms of the use of executable files, the Government has introduced no evidence that PFC Manning had knowledge that by using Wget, he was exceeding his authorized access.

#### **D. The Government Has Not Introduced Evidence of Its Own "Circumvention" Theory**

34. The Government alleges that PFC Manning's use of "unauthorized software"—namely Wget—enabled him to rapidly download information. The fact that Wget rapidly downloads information has, in turn, led the Government to concoct a ridiculous "circumvention" argument whereby it alleges that PFC Manning circumvented the "normal" way of downloading information, thus making his action a computer crime within the meaning of 18 U.S.C. §1030.<sup>7</sup>

35. The circumvention argument is a complete red herring.<sup>8</sup> The Government's theory is that the use of "unauthorized software" can convert what is otherwise authorized access into "exceeds authorized access" within the meaning of section 1030. That unauthorized software in this case happens to be Wget. However, the unauthorized software could be anything, including an unapproved (and more recent) version of an approved program. So, for instance, if PFC Manning had downloaded the cables in an unapproved version of Excel, under the Government's view, he would still have exceeded his authorized access. Nothing turns on how fast or slow the download speed was—the crux of the Government's argument is the use of unauthorized software.

36. The Government now seeks to establish that the "normal" way of downloading information would be to manually press "click, open, and save" and that PFC Manning somehow by-passed or circumvented the process in contravention of Net-Centric Diplomacy access restrictions. The Defense believes that the Government has adopted this nomenclature to make it sound more like what PFC Manning did was hacking<sup>9</sup> or a computer crime under 18 U.S.C. §1030—when in reality it is clear that, at most, it is an Article 92 violation for the use of unauthorized software.

37. The Government has not introduced evidence that "click, open and save" was the normal way of downloading information on a SIPRnet computer. Indeed, analysts testified that they would often export large volumes of information using various tools, to include Excel. They would do this using an "export" function, not "click, open and save." See e.g. Testimony of CPT Fulton (explaining that PFC Manning was tasked to export SIGACTS into Excel to create a work product); Testimony of CW2 Balonek (explaining the use of Excel to import multiple amounts of points at the same time). Mr. Maderas, who was in PFC Manning's brigade, testified that he did not receive any training either at Fort Drum or during the deployment on how one had to download information from the SIPRNET. He testified that there was no formal guidance or statement that analysts had to download information in a particular way—specifically by using "click, open, save." He also testified that analysts often used Excel, which essentially automated the "click, open, save" function and allowed analysts to export large documents without having to manually "click, open and save." In using Excel, Mr. Maderas testified that the automated

<sup>7</sup> This argument is reminiscent of that advanced in *Douglass* where the plaintiff alleged that the defendant's exceeded their authorized access because they used "extraordinarily large" unauthorized storage devices to download information. Although not explicitly addressed in the case, the implication appears to be that the defendants were able to download more information than they otherwise would have been able to owing to the "extraordinarily large" storage devices (much like the Government's argument that PFC Manning was able to download much faster than he otherwise would have been able to do).

<sup>8</sup> Not surprisingly, there is not one case that the Defense was able to locate where the prosecution advanced a theory as attenuated as this.

<sup>9</sup> Agent Shaver testified that Wget is not synonymous with hacking and is just a "tool" that is used in a variety of contexts. In fact, Agent Shaver testified that he used Wget as part of his investigation to replicate the downloads that he identified from his forensic examination. See Testimony of Agent Shaver.



process was permitted and there was never anybody who told him he could not use an automated process. *See* Testimony of Mr. Maderas. Additionally, COL Miller testified that his Brigade did not put out any guidance on how soldiers had to download information on the SIPRNET and stated that there was no “click, open, save” requirement to download information. *See* Testimony of COL Miller.

38. Nor has the Government introduced evidence the Net-Centric Diplomacy database specifically was designed such that a user had to, *as an access restriction*, use the “click, open and save” method of downloading information. Mr. Wisecarver testified that he was not familiar with the design of Net-Centric Diplomacy (indeed, its design was outsourced to a private company). Accordingly, the Government has not introduced any evidence that it was a deliberate design feature of Net-Centric Diplomacy not to have a built-in mechanism for the automated downloading of cables. The lack of a technical feature to facilitate something is not at all indicative of an access restriction.<sup>10</sup> Moreover, the fact that Net-Centric Diplomacy was intended to facilitate “sharing of information” belies any argument that it was intended to have some sort of nonsensical “click, open and save” requirement (as such a requirement would actually inhibit the sharing of information). *See* Testimony of Mr. Wisecarver (indicating that there were no technical restrictions on access because the primary purpose of Net-Centric Diplomacy was information sharing).

39. Even if “click, open and save” were the normal way of downloading information on Net-Centric diplomacy and even if it were designed as some sort of access restriction, the Government has not established that the use of Wget by-passed this method. Indeed, Agent Shaver testified that Wget simply “automated” the process, it did not change it. *See* Testimony of Agent Shaver (noting that Wget did the “click, open, save” in an automated fashion). And, as indicated above, Mr. Wisecarver testified that there was no express prohibition on the Net-Centric Diplomacy database that warned that an automated downloading of information was not permitted. Any access restrictions, to the extent that they may have existed, did not originate with the Department of State, but rather were entrusted to the various government agencies that used Net-Centric Diplomacy. *See* Testimony of Mr. Wisecarver.

### CONCLUSION

40. It is worth noting that the Government has adopted multiple theories of “exceeds authorized access” during the course of this proceeding. If the Government cannot even figure out what the objectionable conduct is which constitutes “exceeding authorized access” how can Soldiers be expected to know which actions are considered to be a “computer crime” and which actions are not? In other words, how could PFC Manning have knowingly exceeded authorized access at the time of the alleged offense if the Government did not even identify what conduct it considered criminal until it failed in its first attempt to state an offense? The fact that the Government is

---

<sup>10</sup> Consider, for instance, earlier versions of the Program Microsoft Word. Older versions of word did not have a function for “pdf”-ing documents (thus, one had to manually pdf a document). This was not indicative of a deliberate design *not* to permit something—i.e. it was not an access restriction. It was simply a feature that Word did not at the time possess.



clinging to a theory which hinges exclusively on the use of an apparently unauthorized program to ground imprisonment for 10 years shows just how weak this charge is.

41. There is not one case—not one—where any court in this country has premised criminal liability on a theory akin to the one the Government is advancing today. That fact alone speaks volumes. Consider, at base, what the Government is saying: the accused had authorized access to the database in question; the accused had authorized access to the information in question; the accused was entitled to download as much information as he wanted; but the accused used the wrong program to download that information. It would be a sad day indeed if a decade in jail could hinge exclusively on what program an accused used to download information he was otherwise entitled to access and otherwise entitled to download.

42. Accordingly, the Defense requests that this Court grant the R.C.M. 917 motion dismissing Specification 13 of Charge II.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'David E. Coombs', with a long horizontal flourish extending to the right.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)  
)  
) **DEFENSE MOTION FOR**  
) **DIRECTED VERDICT:**  
) **SPECIFICATION 16 OF**  
) **CHARGE II (THE USF-I**  
) **GLOBAL ADDRESS LIST)**

) DATED: 4 July 2013  
)

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty for Specification 16 of Charge II.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

3. In Specification 16 of Charge II, the Government alleges that PFC Manning stole or knowingly converted the United States Forces Iraq (USF-I) Microsoft Outlook and SharePoint Exchange Server Global Address List (GAL). The Government has not presented evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of Specification 16 of Charge II.

4. The Defense adopts and incorporates by reference the arguments made in its Motion for Directed Verdict: Charge II, Specifications 4, 6, 8, 12 (18 U.S.C. §641 Offenses) (Defense §641 Motion).<sup>1</sup> In particular, the Defense notes that the Government has not charged that PFC Manning stole or converted "information" contained within the USF-I GAL or that PFC Manning stole or converted "a copy" of the USF-I GAL. This omission is significant both because it changes the identity of the item allegedly stolen or converted and its valuation. For the reasons identified the Defense §641 Motion, and for the additional reasons outlined below, the Defense requests that this Court enter a finding of not guilty.

<sup>1</sup> It is suggested that the Court read Defense §641 Motion prior to reading this motion.

5. The Government has adduced forensic evidence that email addresses containing the term “.mil” were found in the unallocated space in PFC Manning’s personal Macintosh computer. See Testimony of Mr. Johnson. The Government has provided absolutely no evidence that these “.mil” addresses were, in fact, the USF-I GAL which it alleges PFC Manning stole or converted. See Charge Sheet (“In that Private First Class Bradley E. Manning, U.S. Army, did, at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, steal, purloin, or knowingly convert to his use or the use of another, a record or thing of value of the United States or of a department or agency thereof, to wit: *the United States Forces - Iraq Microsoft Outlook / SharePoint Exchange Server global address list* belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S. Code Section 641, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.”) (emphasis added).

6. The Government called no witnesses to testify that they compared the addresses found in the unallocated space of PFC Manning’s computer to the USF-I GAL as it existed on a certain date. See Stipulation of Expected Testimony of SA Williamson (“... revealed a large text file that *appeared to be* an extract of a Microsoft Exchange GAL” (emphasis added); “I did not contact any individual who could have given me the actual Iraq GAL, nor did I compare the data in the files recovered from the above files with the actual Iraq GAL.”). Without any such evidence, the Government has introduced no evidence that would tend to establish that PFC Manning stole or converted the USF-I GAL.

7. More importantly, the Government’s own witness testified that the USF-I GAL contained 160,000 email addresses and that the number of email addresses found in the unallocated space of PFC Manning’s computer totaled 24,000. See 17 June 2013 Testimony of Chief Nixon. When Chief Nixon was called to testify a second time, he testified that what he viewed on PFC Manning’s computer was not the USF-I GAL. See 28 June 2013 Testimony of Chief Nixon. Instead, Chief Nixon testified that he believed (though did not verify) that the .mil addresses on PFC Manning’s computer were part of the Division GAL. *Id.* The testimony from Chief Nixon definitively proves that whatever was on PFC Manning’s computer, it was not the USF-I GAL.

8. Perhaps the Government intends to argue that PFC Manning stole or converted *part* of the USF-I GAL or that PFC Manning stole or converted the Division GAL. However, the Government has not charged PFC Manning with stealing or converting *part* of the USF-I GAL or with stealing or converting the Division GAL—it has charged him with stealing *the* USF-I GAL itself. See Charge Sheet. Stealing or converting the USF-I GAL and stealing or converting the Division GAL are two different offenses, both in terms of the identity of the item actually stolen or converted and its valuation. See *United States v. Wilkins*, 1973 WL 14267, \*639 (ACMR 1972) (evidence of theft of wallet did not establish that the wallet’s contents were \$75.00 as charged; a variance was not permitted since this would change the “nature of the offense charged”); *United States v. Marshall*, No. 08-0779 (C.A.A.F. 2009) (escaping from the custody of one SSG Fleming was a different offense than escaping from the custody of CPT Kreitman). Accordingly, since the Government’s own evidence definitively shows that what was on PFC Manning’s computer was *not* the USF-I GAL as it existed at the time of the alleged offense, the

Government has failed to introduce any evidence that PFC Manning stole or converted the USF-I GAL.

9. Further, the only evidence adduced as to PFC Manning's stealing or converting of what "looks like" the USF-I GAL<sup>2</sup> is that evidence of ".mil" email addresses were found on the unallocated space on PFC Manning's computer. The Government, through its forensic experts, has established that unallocated space means, in laymen's terms, deleted space on the computer. Mr. Johnson testified that most likely these email addresses were something that the user put on the computer and then subsequently deleted. See Testimony of Mr. Johnson. In other words, to the extent that a part of a GAL—(Brigade, Division, or USF-I) may have been located on PFC Manning's computer, the Government's proof shows that it was deleted.

10. The Government has not adduced any evidence that the .mil addresses on the unallocated/deleted space on PFC Manning's computer were transmitted to anyone, much less anyone not authorized to receive it. In particular, the Government has not presented any evidence that the .mil addresses were transmitted by PFC Manning to WikiLeaks. The Government has also not adduced any evidence that WikiLeaks published any of the .mil addresses.

11. The Government has not adduced any evidence that PFC Manning was not permitted to look at, save, or download the .mil addresses. The Government has not established that there was any prohibition placed on PFC Manning, or any other individual, on accessing or downloading the .mil addresses. Indeed, the Government's own witnesses testified that there was no rule or directive stating that soldiers were not permitted to access or download .mil addresses from any GAL. See Testimony of CW4 Rouillard. Similarly, CW2 Balonek testified that there was no prohibition against downloading .mil addresses from any GAL. As well, in his Stipulation of Expected Testimony, SA Williamson stated, "The DoD warning banner and legal notice did not explicitly prohibit the downloading of email addresses. I am not aware of any restriction or guidance that precludes one from downloading email addresses from Outlook." See Stipulation of Expected Testimony of SA Williamson. The Government has therefore not established that, to the extent that a GAL (not the USF-I GAL) was at some point in time in PFC Manning's possession, such possession was somehow "wrongful." See Appellate Exhibit 410 ("To 'steal' means to wrongfully take money or property belonging to the United States government with the intent to deprive the owner of the use and benefit temporarily or permanently. ... 'Wrongful' means without legal justification or excuse.).

12. The Government has not adduced any evidence that, to the extent that PFC Manning may have downloaded a GAL, he acted "with the intent to deprive the government of the use and benefit of the records." See Appellate Exhibit 410. The fact that .mil addresses were found in the unallocated space (i.e. the fact that the .mil addresses were deleted) and there is no evidence that the .mil addresses were ever transmitted to anyone demonstrates a *lack of intent* to deprive the government of the use and benefit of the records.

---

<sup>2</sup> But, as established above, could not be the *actual* USF-I GAL because there were far too few email addresses on PFC Manning's computer for it to be the USF-I GAL.

13. The Government has not adduced evidence that, to the extent that PFC Manning may have downloaded and saved .mil addresses, that such actions constitute “stealing” or “converting” of the USF-I GAL within the meaning of 18 U.S.C. §641.

14. Stealing means “to wrongfully take money or property belonging to the United States government with the intent to deprive the owner of the use and benefit temporarily or permanently.” “Wrongful” is defined as “without legal justification or excuse.” See Appellate Exhibit 410. As discussed above, the Government has provided no evidence that PFC Manning “wrongfully” possessed the .mil addresses. Further, the Government has adduced no evidence that the government was deprived of the use or benefit of the .mil addresses. For instance, the Government has adduced no evidence that PFC Manning’s alleged actions in downloading the .mil addresses caused the .mil addresses to not be accessible to others or that the government was no longer able to use the .mil addresses. CW4 Rouillard testified that there was no impact on U.S. government resources by the downloading of the .mil addresses. See Testimony of CW4 Rouillard. CW4 Nixon testified that the USF-I GAL was always operational, there were never any problems with it caused by PFC Manning’s alleged downloading of .mil addresses. See 17 June 2013 and 28 June 2013 Testimony of CW4 Nixon. CW4 Nixon also testified that there were never any instructions issued by the U.S. government not to use the USF-I GAL or any portion thereof. *Id.*

15. Similarly, the Government has not introduced any evidence that PFC Manning wrongfully converted the USF-I GAL to his own use or to the use of someone else. As stated in the Appellate Exhibit 410, “Conversion may include the misuse or abuse of property. It may reach use in an unauthorized manner or to an unauthorized extent of property placed in one’s custody for limited use. Not all misuse of government property is a conversion. The misuse must seriously and substantially interfere with the United States government’s property rights.” See Appellate Exhibit 410. In *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (per curiam), the court explained that “[t]he cornerstone of conversion is the unauthorized exercise of control over property in such a manner that *serious interference* with ownership rights occurs.” 56 F.3d at 1420 (emphasis in original). *Collins* involved a Section 641 prosecution of a technical analyst at the Defense Intelligence Agency who used the agency’s classified computer system to create and maintain hundreds of documents relating to the analyst’s ballroom dance activities. *Id.* at 1418. In the Section 641 prosecution, the Government alleged that the defendant converted, among other things, the agency’s computer time and storage space.<sup>3</sup> *Id.* The court held that there was insufficient evidence to support the charge relating to conversion of computer time and storage because the Government did not prove that the defendant’s use of the system for non-work related tasks seriously interfered with the Government’s property rights in that system:

[T]he government did not provide a shred of evidence in the case at bar that [defendant] seriously interfered with the government’s ownership rights in its computer system. While [defendant] concedes he typed in data and stored information on the computer regarding his personal activities, no evidence exists that such conduct prevented him or others from performing their official duties on the computer. The government did not even attempt to show that [defendant’s] use of the computer prevented agency personnel from accessing the computer or

<sup>3</sup> Notably, the prosecution did not allege that the defendant in that case stole or converted the *computer* itself.

storing information. Thus, [defendant's] use of the government computer in no way seriously interfered with the government's ownership rights.

*Id.* at 1421. Here, the Government has not introduced evidence that PFC Manning released the .mil addresses he allegedly possessed to WikiLeaks or to anyone else not authorized to receive it. The Government has adduced no evidence that, to the extent that PFC Manning may have ever had possession of the .mil addresses, he did *anything* with the .mil addresses, much less anything that seriously and substantially interfered with the United States government's property interest in the USF-I GAL. The Government has not introduced evidence, for instance, that a large number of the ".mil" addresses on the list received spam or were the subject of phishing scams. In short, the Government has introduced no evidence that PFC Manning either stole or converted the USF-I GAL (or any GAL) within the meaning of 18 U.S.C. §641.

16. Viewed in the light most favorable to the Government, the evidence could show that PFC Manning lawfully downloaded .mil addresses from what appears to be the Division GAL and subsequently deleted the document. This would be equivalent to, say, an attorney downloading the AKO addresses of other attorneys in the JAG Corps, doing nothing with that information, and then subsequently deleting that information. The Government's own witness, CW4 Rouillard, testified that this was perfectly acceptable. *See* Testimony of CW4 Rouillard. The information cannot be regarded to have been "stolen" or "converted" where the original accessor had authorization to download the information, did not transmit the information, and subsequently deleted the information.

17. Further, the Government has introduced no relevant evidence of valuation. It did elicit general testimony about the potential for spearfishing if email addresses are released, but did not put a monetary value on this.<sup>4</sup> Indeed, it withdrew its proffer of CW4 Rouillard as an expert on value. At one point in CW4 Rouillard's testimony, the Government proffered that the "United States is not arguing that value is measured in dollar amounts." Under section 641, the Government must establish value *in dollar amounts*. It cannot present generalized assertions that .mil email addresses have value. It must establish that the particular email addresses that PFC Manning is alleged to have stolen or converted had a value in excess of \$1000 at the time of the alleged offenses.

18. The Government has not established a legitimate "cost of production" for the copy of the email addresses that PFC Manning allegedly downloaded. For the reasons identified in the Defense's Motion for a Directed Verdict on the remaining §641 offenses, it is clear that to the extent that PFC Manning stole or converted anything, it had to be a *copy* of a list. Accordingly, it is a *copy* of the list that must be valued for the purposes of the "cost of production" measure of valuation. *See United States v. DiGiglio*, 538 F.2d 972 (3<sup>rd</sup> 1976) (noting that copies made using government resources, including photocopiers, were "records" for the purposes of §641 and that these copies themselves needed to be valued).

---

<sup>4</sup> Indeed, the Government was correct not to do so, since this is not an acceptable means of valuation. The threat to cyber-security does not demonstrate the monetary value of an item under any acceptable and recognized theory of valuation.

19. Nor has the Government established the value of the email addresses on the thieves' market in May 2009 (the time of the alleged offense). The Government offered Mr. Lewis as an expert on value of all types of information involved in this case, including the GAL. Mr. Lewis is a counter-intelligence expert who has no knowledge of, or expertise in, valuing email addresses. He does not consider himself to be a valuation expert, nor has he ever been asked to value email addresses before. Up until last week, Mr. Lewis maintained that he had no idea why he was being called to testify. Mr. Lewis' valuation "methodology" cannot even be called a methodology. Mr. Lewis did not do relevant research, consider context, or attempt to verify any of his opinions. Accordingly, any testimony from Mr. Lewis regarding the value of a GAL generally does not help establish value of the GAL any more than guessing at the value of the GAL.

20. In *United States v. Wilson*, 284 F.2d 407 (4th Cir. 1960), the defendant was charged with the theft of 72 rifles at a time when Section 641 only required the property to have value in excess of \$100 for a felony conviction. *Id.* at 408. Furthermore, the indictment alleged that the value of the 72 rifles was \$7,500. *Id.* at 407. The Government, however, offered no evidence at trial on the value of the rifles, but the jury still found the defendant guilty on the felony charge. *Id.* at 408. To reach the conclusion that the rifles had value in excess of \$100, the jury only needed to infer that each rifle had a value of at least \$1.39. See *DiGilio*, 538 F.2d at 980-81 (discussing *Wilson*). The Fourth Circuit vacated the defendant's 7 1/2-year sentence because no evidence of the value of the rifles was offered. *Wilson*, 284 F.2d at 408. The *Wilson* Court explained its rationale as follows:

The Government . . . failed to produce any evidence whatsoever as to the value of the stolen weapons. We are asked to take judicial notice that 72 rifles are worth more than \$100.00, but we cannot on the basis of anything in the testimony form a judgment as to value for the purpose of supporting the greater penalty. Nor, in the absence of any proof of value, could the jury be permitted to speculate on this point merely from the appearance of the articles. A fact which distinguishes a violation punishable by imprisonment for not more than one year from a violation punishable by imprisonment for ten years cannot be permitted to rest upon conjecture or surmise. In order to sustain the imposition of the higher penalty, it was as incumbent upon the Government to prove a value in excess of \$100.00 as it was to prove the identity of the defendant as the perpetrator of the crime, or the ownership of the property.

*Id.* The Government's failure to introduce specific evidence on value, rather than generalized assertions of value, is fatal to its 18 U.S.C. §641 claim.

21. Finally, the Government has adduced no evidence that PFC Manning's act of downloading the .mil addresses and then subsequently deleting it is of such a nature to bring discredit to the Armed Forces. The Government cannot rely on the act itself to establish the service discrediting nature of the offense.

CONCLUSION

<sup>2</sup>  
~~20~~ In light of the foregoing, the Defense requests this Court grant the requested R.C.M. 917 motion for Specification 16 of Charge II.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'David E. Coombs', with a stylized, sweeping flourish extending to the right.

DAVID EDWARD COOMBS  
Civilian Defense Counsel



130705-Government Email (Time to File 917 Responses).txt  
From: Fein, Ashden MAJ USARMY MDW (US)  
Sent: Friday, July 05, 2013 3:49 PM  
To: Lind, Denise R COL USARMY (US)  
Cc: 'coombs@armycourtmartrialdefense.com'; Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Bennett, Jessice D SSG USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Mitroka, Katherine F CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); USARMY Ft McNair mdw Mailbox MDW Court Reporters OMB; Raffel, Michael J SFC USARMY (US); Moore, Katrina R MSG USARMY (US)  
Subject: RE: Defense Filing - Government Time to Respond

Ma'am,

The United States requests until COB Thursday, 11 July to file its responses to the Defense's RCM 917 motions. This request is based on multiple factors. The defense filed 44 pages of motions containing many new and old cases that are being relied upon by the defense to argue that the United States presented evidence that is not legally sufficient for RCM 917 purposes. These motions are technical legal arguments, thus requiring extensive research, and not arguments focused on mere insufficiency of evidence related to the elements. Also, the defense appears to be re-litigating the Court's 18 USC 1030 rulings, which require more time to research these issues. Not only does the United States need to thoroughly research these cases and others from all the filings, but also must outline for the Court the witness testimony and approximately 180 prosecution exhibits presented over the past 30 days. Additionally, since we are pushing forward with the defense's case on Monday morning, the United States requests the filing date be COB Thursday, 11 July to allow for the concurrent preparation of the defense's first 10 witnesses.

The above request would give the United States 7 days, including today

Page 1

APPELLATE EXHIBIT 597  
PAGE REFERENCED  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

130705-Government Email (Time to File 917 Responses).txt  
and the  
weekend, to concurrently research and write our responses, prepare for  
the  
first 10 defense witnesses, and participate in the trial next week.

Thank you.

v/r  
MAJ Fein

-----Original Message-----

From: Lind, Denise R COL USARMY (US)  
Sent: Friday, July 05, 2013 11:18 AM  
To: 'coombs@armycourt martialdefense.com'  
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US);  
Bennett, Jessice D SSG USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Mitroka, Katherine F CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); USARMY Ft McNair mdw Mailbox MDW  
Court Reporters OMB; Raffel, Michael J SFC USARMY (US); Fein, Ashden MAJ USARMY MDW (US); Moore, Katrina R MSG USARMY (US)  
Subject: Re: Defense Filing - Government Time to Respond

Government,

By COB today, advise the Court how much time you request to respond to the  
Defense motions in the below email.

D

----- Original Message -----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]  
Sent: Thursday, July 04, 2013 03:37 PM Coordinated Universal Time  
To: Lind, Denise R COL USARMY (US)  
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US);  
Bennett, Jessice D SSG USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Mitroka,

130705-Government Email (Time to File 917 Responses).txt  
Katherine F CPT  
USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); USARMY Ft McNair mdw  
Mailbox  
MDW Court Reporters OMB; Raffel, Michael J SFC USARMY (US); Fein,  
Ashden MAJ  
USARMY MDW (US); Moore, Katrina R MSG USARMY (US)  
Subject: Defense Filing

Ma'am,

Please find attached the following R.C.M. 917 motions:

1. Motion for Directed Verdict: 104 Offense
2. Motion for Directed Verdict: 1030 Offense
3. Motion for Directed Verdict: 641 Offenses (excepting the USF-I  
Global  
Address List)
4. Motion for Directed Verdict: the USF-I Global Address List

The Defense asks that you read the Motion for Directed Verdict for the  
641  
Offenses prior to reading the Motion for Directed Verdict for the GAL  
since  
the latter cross-references the former.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
coombs@armycourt martialdefense.com  
www.armycourt martialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments,  
may  
contain confidential attorney-client information and is intended for  
the  
person(s) or company named. If you are not the intended recipient,  
please  
notify the sender and delete all copies. Unauthorized disclosure,  
copying  
or use of this information may be unlawful and is prohibited.\*\*\*

130705-Government Email (Time to File 917 Responses).txt

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211


Witness List Order  
for the Defense  
Witnesses

7 July 2013

The Defense hereby submits the following order for the first ten witnesses the Defense intends to call in the above-captioned court-martial:

1. CW2 Joshua Ehresman
2. SGT David Sadtler
3. CPT Steven Lim
4. CPT Barclay Keay
5. Ms. Lauren McNamara

6. Col(r) Morris Davis
7. Mr. Cassius Hall
8. Mr. Charles Ganiel
9. Stipulation – Defense Exhibit B
10. Professor Yochai Benkler

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel

APPELLATE EXHIBIT 592  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government Response  
to Defense Motion for  
Directed Verdict:  
Charge II, Specifications  
4, 6, 8, 12, and 16  
(18 U.S.C. § 641)

11 July 2013

### RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion for Directed Verdict: Charge II, Specifications 4, 6, 8, 12 (hereinafter "Defense 641 Motion") and Defense Motion for Directed Verdict: Specification 16 of Charge II (hereinafter "Defense GAL Motion") (collectively "Defense Motions") because the United States has presented evidence for each element of each specification. The United States combines its response to the Defense Motions herein.

### BURDEN OF PERSUASION AND BURDEN OF PROOF

"A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." Rule for Courts-Martial (hereinafter "RCM") 917(d). "The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*

### FACTS

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice. The accused is also charged with causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, UCMJ, eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641 (hereinafter "§ 641"), two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications alleging misconduct in violation of Article 92 of the UCMJ. *See* Charge Sheet.

The accused pleaded guilty by substitutions and exceptions to Specifications 2, 3, 5, 7, 9, 10, 13, 14 and 15 of Charge II. *See* Appellate Exhibit (hereinafter "AE") CDXLIV. The accused did not plead guilty *inter alia*, to Specifications 4, 6, 8, 12, and 16 of Charge II (hereinafter "§ 641 specifications"). *See id.*

### WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States requests that the Court consider the Charge Sheet, Prosecution Exhibits, testimony, and the Appellate Exhibits cited herein.

## LEGAL AUTHORITY AND ARGUMENT

The United States submitted evidence relevant to the § 641 specifications that was admitted. The Defense argues that the United States has failed to satisfy the standard set forth in RCM 917(d). The admitted evidence establishes a reasonable inference that the accused stole and converted the databases and records listed in the § 641 specifications. The Defense arguments that the § 641 specifications constitute fatal variances lack merit because the evidence proves the contents of the databases and the records were stolen or converted. The evidence does not constitute a material variance. Additionally, the Defense had adequate notice and ability to prepare the accused's defense for trial.

### I. EVIDENCE ADMITTED AT TRIAL RELEVANT TO § 641 SPECIFICATIONS

#### A. R.C.M. 917 Background

"The military judge, on motion by the accused or *sua sponte*, shall enter a finding of not guilty of one or more offenses charged after the evidence on either side is closed and before findings on the general issue of guilt are announced if the evidence is insufficient to sustain a conviction of the offense affected." RCM 917(a). The motion by the accused shall state with specificity where the evidence is insufficient to enable the trial counsel to respond to the motion, and the Court shall give each party an opportunity to be heard on the matter. *See* RCM 917(b); RCM 917(c); RCM 917(c), discussion (stating that the military judge ordinarily should permit the trial counsel to reopen the case as to the insufficiency specified in the motion).

A motion for a finding of not guilty "shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." RCM 917(d). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id*; *United States v. Perez*, 40 M.J. 373 (C.M.A. 1994) (upholding the military judge's decision not to enter a finding of not guilty because the testimony of three witnesses, construed in the light most favorable to the prosecution, could reasonably tend to establish the overt act). The standard of "some evidence" required to survive a motion for a finding of not guilty is a low one. *See United States v. Escochea-Sanchez*, 2013 WL 561356 (N-M. Ct. Crim. App. 2013) (concurring with the military judge who "noted repeatedly while hearing argument on the RCM 917 motion [that] the standard for surviving such a motion is very low"); *United States v. Jenkins*, 59 M.J. 893, 898 (A. Ct. Crim. App. 2004) (encouraging trial judges to view the standard used to decide whether to grant a motion for a finding of guilty as a mirror image of the standard used to decide whether to give an instruction on an affirmative defense); *United States v. Athearn*, 1994 WL 711894 (A.F. Ct. Crim. App. 1994) (noting that "[t]he military judge was obviously correct in denying the motion for a finding of not guilty under the low, 'some evidence' standard set out in R.C.M. 917(d)") (quoting RCM 917(d)). Direct or circumstantial evidence satisfies the "some evidence" standard. *See United States v. Parker*, 59 M.J. 195 (C.A.A.F. 2003); *United States v. Varkonyi*, 645 F.2d 453, 458 (5th Cir. 1981).

## B. Relevant Evidence Admitted

Relevant evidence is evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence. Military Rule of Evidence (hereinafter "MRE") 401. Relevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way in a matter at issue. The military judge has the initial responsibility to determine whether evidence is relevant under MRE 401. *See United States v. White*, 69 M.J. 236 (C.A.A.F. 2010). Elements of charged offenses are relevant and defined by the specification. *See* Rule for Courts-Martial 307(c)(3) (defining a specification as a plain, concise, and definite statement of the essential facts constituting the offense charged).

In the Defense Motions, the Defense does not dispute that the Combined Information Database Network Exchange (hereinafter "CIDNE")-Iraq database, CIDNE-Afghanistan database, United States Southern Command (hereinafter "USSOUTHCOM") database, Department of State Net-Centric Diplomacy (NCD) database, and United States Forces- Iraq Microsoft Outlook/SharePoint Exchange Server global address list (hereinafter "USF-I GAL") belonged to the United States or a department or agency thereof. Further, the Court took judicial notice that 18 U.S.C. § 641 was in existence on the dates alleged in Specifications 4, 6, 8, 12 and 16. *See* AE DLXXXVIII; AE DLXXXVIII(a).

The accused was not authorized to give classified information to the WikiLeaks organization. *See, e.g.*, PE 59; PE 60; Testimony of CPT Fulton; Testimony of Special Agent (hereinafter "SA") Mander; Testimony of Ms. Glenn; Testimony of SSgt Hosburgh. The Court took judicial notice that WikiLeaks posted records from the CIDNE-Iraq database, CIDNE-Afghanistan database, and USSOUTHCOM database. AE DLXXXVIII. SA Bettencourt confirmed that WikiLeaks posted the purported Department of State records from the NCD database. *See* PE 76.

### 1. Specification 4 of Charge II

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records." *See* AE CDX. SA David Shaver testified that the accused stole, purloined, or knowingly converted more than 380,000 records from the CIDNE-Iraq database on a Secure Digital (SD) card. *See* Testimony of SA Shaver. SA Shaver testified that these records were stored in a folder entitled "yada.tar.bz2.nc" with the filename "irq\_events.csv." *See id.* The folder entitled "yada.tar.bz2.nc" and its contents were admitted into evidence. *See* Prosecution Exhibit (hereinafter "PE") 92. On 2 November 2010, SA Mark Mander collected this SD card from the home of Ms. Debra Van Aalst, the aunt of the accused. *See* PE 78; PE 113. On 3 November 2010, Ms. Tamara Mairena received this SD card from SA Mander and, on 10 December 2010, released the SD card to SA Shaver for examination. *See* PE 29. This SD card contained a picture of the accused, in addition to more than 380,000 records from the CIDNE-Iraq database. *See* PE 40; PE 113. The SD card was admitted into evidence. *See* PE 92.



The accused admitted to this misconduct to Mr. Adrian Lamo. *See* PE 30. When asked "(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?[,]" the accused admitted "(04:35:31 PM) bradass87: The Gharani airstrike videos and full report, Iraq war event log, the "Gitmo Papers", and State Department cable database . . ." *See id.* at 46.

The United States presented evidence that "the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records." *See* AE CDX. The SD card with which the accused stored the records from the CIDNE-Iraq database contained a document entitled "README.txt." *See* Testimony of SA Shaver. The "README.txt" document was last written on 9 January 2010. *See id.* With this document, the accused identified the contents of the SD card to include the "Iraq and Afghanistan Significant Activities (SIGACTs) between 0000 on 01 JAN 2004 and 2359 on 31 DEC 2009." *See* PE 42. The accused also recommended that the recipient "might need to sit on this information, perhaps 90-180 days, to figure out how best to release such a large amount of data, and to protect source." *See* PE 42. Mr. Troy Moul, the accused's instructor at Advanced Individual Training (AIT), testified that, during AIT, the accused received substantial training on the definition, marking, and proper handling of classified information. *See* Testimony of Mr. Moul. The PowerPoint slides that the accused received at AIT were admitted into evidence. *See* PE 52. The accused also executed several Non-Disclosure Agreements (NDAs), whereby the accused acknowledged his responsibility not to disclose classified information to unauthorized persons. These NDAs were admitted into evidence. *See* PE 59; PE 60. Every member of the accused's unit, who testified, stated that Soldiers were not authorized to remove classified information from the Sensitive Compartmented Information Facility (SCIF). *See* Testimony of CPT Casey Fulton; Testimony of CW2 Kyle Balonek; Testimony of COL David Miller.

Executive Order (EO) 13526, which the Court took judicial notice of, verifies that classified information may not be removed from official premises without proper authorization. *See* EO 13526 § 4.1(d); AE CDX. EO 13526 also states that "[i]nformation may be originally classified only if... (2) the information is owned by, produced by or for, or is under the control of the United States Government." *See* EO 13526 §1.1. Army Regulation (AR) 380-5, paragraph 2-8, which the Court took judicial notice of, also states that "U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of, the United States Government." *See* AR 380-5 at ¶ 2-8.

The accused made many admissions to Mr. Lamo that establish a reasonable inference that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. A sampling of the relevant statements, in chronological order, is set forth below:

- i. "(12:22:49 PM) bradass87: the air gap has been penetrated , . . =L[.]" PE 30, at 8.
- ii. "(12:26:09 PM) bradass87: lets just say \*someone\* i know intimately well, has been penetrating US classified networks, mining data like the ones described... and been transferring that data from the classified networks over the "air gap" onto a commercial network computer... sorting the data, compressing it, encrypting it, and

uploading it to a crazy white haired aussie who can't seem to stay in one country very long =L[.]” PE 30, at 8.

- iii. “(1:34:11 PM) bradass87: waiting to redeploy to the US, be discharged... and figure out how on earth im going to transition  
(1:34:45 PM) bradass87: all while witnessing the world freak out as its most intimate secrets are revealed[.]” PE 30, at 10.
- iv. “(03:07:01 PM) bradass87: i just... couldnt let these things stay inside of the system... and inside of my head...[.]” PE 30, at 26.
- v. “(02:23:25 PM) bradass87: i could’ve sold to russia or china, and made bank?  
(02:23:36 PM) info@adrianlamo.com: why didn’t you?  
(02:23:58 PM) bradass87: because it’s public data  
(02:24:15 PM) info@adrianlamo.com: i mean, the cables  
(02:24:46 PM) bradass87: it belongs in the public domain  
(02:25:15 PM) bradass87: information should be free  
(02:25:39 PM) bradass87: it belongs in the public domain[.]”

PE 30 (ellipses in original).

The United States presented evidence that “the records were of a value greater than \$1,000.” See AE CDX. The parties entered into a stipulation of expected testimony for Mr. Wyatt Bora. See PE 115. This evidence confirms the following:

- i. “In 2007, the program spent approximately \$900,000 on data management in Iraq. In 2008, the program spent approximately \$1,000,000 on data management in Iraq. In 2009, the program spent approximately \$4,200,000 on data management in Afghanistan and \$1,800,000 on data management in Iraq. In 2010, the program spent approximately \$3,600,000 on data management in Afghanistan. In 2011, the program spent approximately \$3,000,000 on data management in Afghanistan and \$570,000 on data management in Iraq. In 2012, the program spent approximately \$5,000,000 on data management in Afghanistan. These data management costs are directly associated with keeping the data useable on the classified networks.”
- ii. “In 2005, the program spent approximately \$1,100,000 for development and testing in Iraq and \$1,800,000 in development and testing in the Continental United States (CONUS). In 2006, the program spent approximately \$1,770,000 for development and testing in Iraq and \$790,000 in development and testing in CONUS. In 2007, the program spent approximately \$1,320,000 for development and testing in Iraq and \$1,810,000 in development and testing in CONUS. In 2008, the program spent approximately \$950,000 for development and testing in Afghanistan, \$2,690,000 for development and testing in Iraq, and \$3,610,000 in development and testing in CONUS. In 2009, the program spent approximately \$2,760,000 for development and testing in Afghanistan, \$3,280,000 for development and testing in Iraq, and \$5,500,000 in development and testing in CONUS. In 2010, the program spent

approximately \$4,200,000 for development and testing in Afghanistan, \$2,650,000 for development and testing in Iraq, and \$4,980,000 in development and testing in CONUS.”

- iii. “In 2007, the program spent approximately \$720,000 on hardware in Iraq. In 2008, the program spent \$560,000 on hardware in Afghanistan and \$190,000 on hardware in Iraq. In 2009, the program spent approximately \$1,660,000 on hardware in Afghanistan and \$520,000 on hardware in Iraq. In 2010, the program spent \$760,000 on hardware in Afghanistan. In 2011, the program approximately spent \$180,000 on hardware in Afghanistan. In 2012, the program spent approximately \$3,680,000 on hardware in Afghanistan.”
- iv. “In 2005, the program spent approximately \$1,100,000 for Iraq training. In 2006, the program spent approximately \$1,180,000 for Iraq training and \$480,000 for CONUS training. In 2007, the program spent approximately \$2,570,000 for Iraq training and \$200,000 for CONUS training. In 2008, the program spent approximately \$1,850,000 for Afghanistan training, \$5,220,000 for Iraq training, and \$1,550,000 for CONUS training. In 2009, the program spent approximately \$5,360,000 for Afghanistan training, \$6,370,000 for Iraq training, and \$3,660,000 for CONUS training. In 2010, the program spent approximately \$8,140,000.00 for Afghanistan training, \$5,150,000 for Iraq training, and \$3,320,000 for CONUS training. In 2011, the program spent approximately \$18,410,000 for Afghanistan training, \$2,650,000 for Iraq training, and \$6,150,000 for CONUS training. In 2012, the program spent approximately \$8,790,000 for Afghanistan training and \$2,740,000 for CONUS training.”
- v. “From 2005 through 2012, the CIDNE program spent approximately \$181,160,000 on contracted support required to run the program, to include development, training, data management, and hardware. In addition, from 2005 through 2012, the program spent approximately \$5,434,800.00 on program management support, to include government testing, administrative oversight, and research and development.”

*See id.* Mr. Danny Lewis also testified that the value of these records is greater than \$1,000. *See* Testimony of Mr. Lewis.

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” *See* AE CDX. COL Miller, the Brigade Commander for 2d Brigade Combat Team (BCT), 10th Mountain Division, testified that he was “stunned” when he learned of the accused’s misconduct because the last thing he anticipated was an internal security breach from one of their own. *See* Testimony of COL Miller. COL Miller testified that the impact to the brigade’s morale was significantly affected. *See id.* Before learning of the accused’s misconduct, COL Miller explained that the brigade’s morale was at its highest point since he took command because many of the Soldiers assigned to the unit had deployed multiple times and, having been tasked as the first BCT responsible for drawdown in Iraq, the Soldiers were seeing the fruits of their labor over the past ten years coming to fruition. *See id.* COL Miller testified that the accused’s misconduct was prejudicial to good order and

discipline because the atmosphere throughout the brigade as a result of the accused's misconduct was like that of a "funeral"—full of anger, sadness, grief, and frustration. *See id.* COL Miller also testified that the impact to the brigade's trust with one another was significantly affected. *See id.* COL Miller testified that trust is critical in theater and, similar to how Soldiers must trust one another in a combat patrol, trust is crucial among Soldiers in the S-2 section for safeguarding classified information. *See id.* The accused's acts as described by COL Miller, to include, *inter alia*, the harm to trust among Soldiers, caused discredit. Furthermore, the accused's admission of the world's awareness of the records he compromised caused discredit. *See* PE 30.

Lastly, Mr. Jason Milliman testified that having a large amount of information stored on one's desktop caused problems with the Distributed Common Ground System-Army (DCGS-A) computers in theater. *See* Testimony of Mr. Milliman. Mr. Chad Madaras, a former Soldier who worked on the day shift and shared a classified government computer with the accused in theater, testified that he observed the size of the accused's desktop and testified that it was large and filled with many items. *See* Testimony of Mr. Madaras. Mr. Madaras testified that he experienced many problems with his computer after the accused's shift completed. Mr. Madaras testified that he lost about two hours of work each time he experienced problems with his computer. *See id.*

## *2. Specification 6 of Charge II*

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the Combined Information Network Exchange Afghanistan database containing more than 90,000 records." *See* AE CDX. SA Shaver testified that the accused stole, purloined, or knowingly converted more than 90,000 records from the CIDNE-Afghanistan database on a SD card. *See* Testimony of SA Shaver. SA Shaver testified that these records were stored in a folder entitled "yada.tar.bz2.nc" with the filename "afg\_events.csv." *See* Testimony of SA Shaver. The filename "afg\_events.csv" was last written on 8 January 2010. *See id.* This SD card contained a picture of the accused, in addition to more than 90,000 records from the CIDNE-Afghanistan database. *See* PE 40; PE 113. The SD card was admitted into evidence. *See* PE 92.

The United States presented evidence that "the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records." *See* AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

The United States presented evidence that "the records were of a value greater than \$1,000." *See* AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II. Mr. Lewis also testified that the value of these records is greater than \$1,000. *See* Testimony of Mr. Lewis.

The United States presented evidence that "under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature

to bring discredit upon the armed forces.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

### *3. Specification 8 of Charge II*

The United States presented evidence that “at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else’s use, to wit: a United States Southern Command database containing more than 700 records.” See AE CDX. SA Shaver testified that PE 83 consists of a summary of Intelink logs showing that the accused, on 8 March 2010, used Wget to retrieve more than 700 records from the United States Southern Command database accessible through the Joint Task Force–Guantanamo (JTF-GTMO) Detainee Assessment Branch website on Intellipedia. See Testimony of SA Shaver; PE 82; PE 83. SA Shaver explained that the number “200” in PE 83 means that the accused successfully executed Wget to retrieve the “DocumentID” of records relating to JTF-GTMO detainees. Mr. Jeffrey Motes confirmed that the records in the United States Southern Command database were stored by “DocumentID” and that the above database consisted of over 700 records. See PE 131.

The accused further admitted to his misconduct to Mr. Lamo. See PE 30. When asked “(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?[,.]” the accused admitted “(04:35:31 PM) bradass87: The Gharani airstrike videos and full report, Iraq war event log, the “Gitmo Papers”, and State Department cable database[.]” See *id.* at 46.

The United States presented evidence that “the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

The United States presented evidence that “the records were of a value greater than \$1,000.” See AE CDX. The stipulation of Mr. Motes explained, in detail, the steps necessary to prepare the records from the United States Southern Command database. See PE 131. Mr. Motes confirmed that it took, on average, 80-90 working hours to create each of the 700 records the accused stole and that the most detainee assessments created in one year was approximately 520. See *id.* Mr. Motes also confirmed that the lowest ranking Servicemember responsible for creating these records was E-4 and the lowest ranking government employee responsible for creating these records was GS-12. The Court took judicial notice of the salaries for persons of these ranks. See AE DLXXXVIII. Mr. Lewis also testified that the value of these records is greater than \$1,000. See Testimony of Mr. Lewis.

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

#### 4. Specification 12 of Charge II

The United States presented evidence that “at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else’s use, to wit: the Department of State NCD database containing more than 250,000 records.” See AE CDX. The Department of State firewall server logs show an incredible amount of activity between the accused’s classified government computer and the NCD database. See PE 159. SA Shaver testified that he recovered a folder from the accused’s computer with Department of State cables. See Testimony of SA Shaver; See PE 12. SA Shaver explained how the accused converted the cables into Comma Separated Value (CSV) format with Base64 encryption. See Testimony of SA Shaver. The excel spreadsheet retrieved from the accused’s computer shows that the accused was cataloguing the theft of 251,287 Department of State diplomatic cables and was admitted into evidence. See PE 102. SA Bettencourt retrieved 251,287 purported Department of State diplomatic cables from WikiLeaks. See PE 76. The accused admitted this misconduct in chats with Mr. Lamo, stating: “(02:16:48 AM) info@adrianlamo.com: embassy cables? (02:16:54 AM) bradass87: yes (02:17:00 AM) bradass87: 260,000 in all[.]” See PE 30, at 34.

The United States presented evidence that “the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II. Additionally, Mr. Charley Wisecarver testified that each diplomatic cable in the NCD database displayed a warning banner. See Testimony of Mr. Wisecarver. See PE 169(c); PE 170(c); PE 171(c); PE 172(c); PE 173(c); PE 175(c); PE 176(c); PE 177(c). Further, and in addition to those statements listed in Specification 4 of Charge II, the accused made many additional admissions to Mr. Lamo establish a reasonable inference that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. These admissions, in chronological order, are set forth below:

- i. “(12:52:33 PM) bradass87: Hilary Clinton, and several thousand diplomats around the world are going to have a heart attack when they wake up one morning, and finds an entire repository of classified foreign policy is available, in searchable format to the public... =L”
- ii. “(01:52:30 PM) bradass87: funny thing is... we transferred so much data on unmarked CDs...  
(01:52:42 PM) bradass87: everyone did... videos... movies... music  
(01:53:05 PM) bradass87: all out in the open  
(01:53:53 PM) bradass87: bringing CDs too and from the networks was/is a common phenomeon  
(01:54:14 PM) info@adrianlamo.com: is that how you got the cables out?  
(01:54:28 PM) bradass87: perhaps  
(01:54:42 PM) bradass87: i would come in with music on a CD-RW  
(01:55:21 PM) bradass87: labelled with something like “Lady Gaga”... erase the music... then write a compressed split file  
(01:55:46 PM) bradass87: no-one suspected a thing

(01:55:48 PM) bradass87: =L kind of sad  
(01:56:04 PM) info@adrianlamo.com: and odds are, they never will  
(01:56:07 PM) bradass87: i didnt even have to hide anything  
(02:00:12 PM) bradass87: everyone just sat at their workstations... watching music videos / car chases / buildings exploding... and writing more stuff to CD/DVD... the culture fed opportunities"

- iii. "(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?  
(04:35:31 PM) bradass87: The Gharani airstrike videos and full report Iraq war event log the "Gitmo Papers" and State Department cable database"

PE 30 (ellipses in original) (emphasis added).

The United States presented evidence that "the records were of a value greater than \$1,000." See AE CDX. Mr. Wisecarver testified that the technicians responsible for maintaining the NCD database earned approximately \$70,000 annually and that the yearly maintenance of the database "well" exceeded \$1,000. See Testimony of Mr. Wisecarver. Mr. Lewis also testified that the value of these records is greater than \$1,000. See Testimony of Mr. Lewis.

The United States presented evidence that "under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces." See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

##### *5. Specification 16 of Charge II*

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the United States Forces- Iraq Microsoft Outlook/SharePoint Exchange Server global address list." See AE CDX. On 7 May 2010, WikiLeaks requested via Twitter email addresses for military personnel. See PE 31. SA Alfred Williamson confirmed that the accused, on 11 May 2010, searched Google for "global address list Microsoft excel macro." See PE 143. The accused conducted this search on the unclassified government computer in the supply office at Forward Operating Base (FOB) Hammer, Iraq. See *id.* SA Williamson found the accused's profile on this government computer, and SSG Peter Bigelow, the other user of this computer, confirmed that he "did not know what the Global Address List was." See PE 142. SA Williamson found the text file entitled "blah.txt" on this computer which contained 74,000 exchange-formatted email addresses and names of unit, ranks, and sections of personnel. See PE 143.

The United States presented evidence that "the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records." See AE CDX. SA Williamson confirmed that "on login to the computer by a user, the computer was set to display a Department of Defense warning banner and legal notice." PE 143. Further, Mr. Moul testified that the accused received Operational Security (OPSEC) training at AIT, which instructed the accused not to disclose this type of information to unauthorized persons. See

Testimony of Mr. Moul. The tasker created by the accused to “exfiltrate” the global address list further supports that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. See Testimony of Mr. Johnson; PE 122. Digital remnants of the USF-I GAL were located on the accused’s personal computer. *Id.*

The United States presented evidence that “the records were of a value greater than \$1,000.” See AE CDX. Mr. Lewis also testified that the value of these records is greater than \$1,000. See Testimony of Mr. Lewis. CW4 Nixon testified that the software and hardware pieces required to operate the USF-I GAL cost between tens of thousands and over a million dollars. See Testimony of CW4 Nixon. CW4 Nixon also testified that the USF-I GAL could not operate without the software and hardware. See *id.*

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” See AE CDX. Evidence supporting this element came from the testimony of COL Miller, as set forth above in Specification 4 of Charge II. The Defense does not allege that the United States has failed to provide evidence that the accused’s conduct is prejudicial to good order and discipline. See Defense GAL Motion ¶ 21. The analysis for a finding of prejudice to good order and discipline is conducted separately from the analysis of whether conduct is service discrediting. See, e.g., *United States v. Davis*, 26 M.J. 445, 448 (C.M.A. 1988). Evidence of both prejudice to good order and discipline and discredit to the service has been admitted. See Part I.B.1, *supra*.

Therefore, based on the above evidence and all reasonable inferences drawn therefrom, the United States satisfied the requirements of RCM 917(d).

### C. Relevance Objection Forfeited Where Not Timely Made

In order to preserve an objection when “the ruling is one admitting evidence” the objecting party must make a “timely objection or a motion to strike” and must state the specific ground of the objection. MRE 103(a)(1); *United States v. Reynoso*, 66 M.J. 208, 210 (C.A.A.F. 2008). Application of 103 and its requirement for a timely objection should be applied practically, not formulaically. See *Reynoso*, 66 M.J. at 210.

In the instant case, the Defense did not object to the evidence detailed in Part I.B as irrelevant. To the extent the Defense believed the admitted evidence regarding the stolen databases did not relate to the § 641 specifications, the Defense should have raised an objection to the evidence’s relevance. The Defense declined to object. Having thus conceded the evidence’s relevance, the Defense cannot claim that “the Government has failed to adduce evidence that [the accused] stole or converted the databases in question.” The Defense Motions’ arguments are not a timely objection because the Defense remained silent about the relevance of the evidence detailed in Part I.B upon its introduction into evidence. *Ford ex rel. Estate of Ford v. Garcia*, 289 F.3d 1283, 1296 (11th Cir. 2002) (“Where a party has the opportunity to object, but remains silent or fails to state the grounds for objection, objections . . . will be waived . . .”) (quotations and citations omitted); *United States v. Wong*, 40 F.3d 1347, 1378-79 (2d Cir. 1994) (holding objection waived where not raised during a sidebar conference despite ample



opportunity); *see also United States v. White*, 25 M.J. 50, 52 (C.M.A. 1987) (deciding the defense forfeited any objection to assailant's identity where defense elicited the identity of the assailant on cross-examination). Therefore, the Defense forfeited any objection about the relationship of the evidence to the *res* of the § 641 specifications.

## II. VARIANCE

The Defense also avers that the admitted evidence constitutes a fatal variance because "information" was not specifically charged. *See* Defense 641 Motion ¶ 9 ("If the Government in this case intended to charge theft of the *information* itself or theft of a *copy* of a record, instead of theft of the database, such a charge must appear in the Charge Sheet.") (emphasis in original). The Defense claim lacks merit because no variance exists. The United States charged that the accused compromised databases, to include the records contained in the databases. *See* Charge Sheet. The United States admitted evidence to provide a reasonable inference the records were stolen and converted. Furthermore, the accused himself referred to the records he asported as "databases" in his chats.

"A variance between pleadings and proof exists when evidence at trial establishes the commission of a criminal offense by the accused, but the proof does not conform strictly with the offense alleged in the charge." *United States v. Allen*, 50 M.J. 84, 86 (C.A.A.F. 1999) (citing *United States v. Lee*, 1 M.J. 15, 16 (C.M.A. 1975)). To prevail on its claim of a fatal variance, the Defense must demonstrate that the variance is material and substantially prejudicial. *United States v. Finch*, 64 M.J. 118, 121 (C.A.A.F. 2006). A variance is material where it "substantially changes the nature of the offense, increases the seriousness of the offense, or increases the punishment of the offense." *United States v. Marshall*, 67 M.J. 418, 420 (C.A.A.F. 2009) (citing *Finch, supra*). A variance is prejudicial where it puts the accused at risk of another prosecution for the same conduct, misleads to the extent that the accused is unable to prepare adequately for trial, or denies the accused the opportunity to defend against the charge. *Id.* (citing *United States v. Teffau*, 58 M.J. 62, 66 (C.A.A.F. 2003)).

### A. US Charged Databases and Records, and those charges include the info in the records

#### 1. Plain meaning of charged terms "database" and "records" includes information

For all § 641 specifications, the accused has been charged with stealing, purloining, or converting a database, to include its records, or the USF-I GAL.<sup>1</sup> The Charge Sheet specifies that the CIDNE-Iraq database contained more than 380,000 records, the CIDNE-Afghanistan database contained more than 90,000 records, the USSOUTHCOM database contained more than 700 records, and the NCD database contained more than 250,000 records. The Defense opines that the United States did not charge the accused with stealing or converting information.

---

<sup>1</sup> In this motion, the United States uses the term "steal" and its variations as synonymous with "stealing" and "purloining." The element of stealth required for "purloining" is not necessary under the specifications at issue because the accused has been charged with stealing, purloining, or converting certain databases and information. *See* Charge Sheet. However, the United States has offered evidence of the stealthiness employed by the accused in compromising the databases. *See* PE 30.

Defense 641 Motion at ¶ 5-6 (stating that a database is “not any way synonymous with the information or records contained therein” and that the United States could have charged the accused with stealing “information”).<sup>2</sup> By the plain meanings of the § 641 specifications, the records include the information contained therein. A database is “a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means.” Black’s Law Dictionary (9th ed. 2009). Similarly, a record is “information that is inscribed on a tangible medium or that, having been stored in an electronic or other medium, is retrievable in perceivable form.” Black’s Law Dictionary (9th ed. 2009). The Charge Sheet informed the accused of the stolen *res* because the Charge Sheet described stolen records, which, by definition, includes the information in those records. See Part III, *infra*; *see, e.g.*, Testimony of Mr. Lewis, Testimony of CW4 Nixon; Testimony of CW4 Rouillard.

The Defense’s reliance on its filing cabinet analogy is misplaced. The United States charged the accused with stealing or converting the databases, which consisted of a collection of records. The databases were contained in servers. In the instant case, the servers are more appropriately comparable to a filing cabinet. While the servers are relevant to valuation as instruments that support the use of the databases, the servers are not the charged databases.

## 2. The accused agrees that “database” and “records” includes information

Moreover, the accused repeatedly referred to the records he compromised as “databases.” See PE 30. The accused also describes the information contained in these databases, writing, “(12:21:24 PM) bradass87: [S]ay . . . a database of half a million events during the Iraq war . . . from 2004 to 2009 . . . with reports, date time groups, lat-lon locations, casualty figures . . . ? or 260,000 state department cables from embassies and consulates all over the world, explaining how the first world exploits the third, in detail, from an internal perspective?” *Id.* at 8 (ellipses in original); *see also id.* at 9 (describing the 9/11 pager messages as a database). The accused further connected a database to the information it contains, noting, “(7:44:01 AM) bradass87: [B]ut once a single piece of information is found . . . then the database can be sifted and sifted and sifted some more, for refinement, so other intelligence functions can get in the act.” *Id.* at 17 (ellipsis in original).

## 3. Information as part of records comports with precedent

Charging records and the information contained therein comports with applicable precedent in criminal law. The contents and information contained in government records determines the criminality of the theft of the records more than the form of the records. See *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), *cert. denied*, 385 U.S. 974 (1966) (“When the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owners should be deemed immaterial.”); *United States v. Lambert*, 446 F.Supp. 890, 894 (D.C. Conn. 1978). Under § 641, the transmission of the information contained in documents is just as larcenous as theft of the documents themselves. *United States*

<sup>2</sup> Specific records, to include birth records and marriage records, are also defined to include information. Black’s Law Dictionary (9th ed. 2009).

v. *Rosner*, 352 F.Supp. 915, 922 (D.C.N.Y. 1972) (noting that the importance of information in documents described in *Botione* applies to § 641 charges).

#### B. United States Presented Evidence of Theft and Conversion

The accused both stole and converted the information he compromised. Relying on dicta, the Defense argues that the United States must prove conversion and demonstrate a serious and substantial interference with its rights in the databases. Defense 641 Motion ¶ 11. The Defense's theory ignores the statutory terms of § 641 and the Charge Sheet's use of the statutory theories of stealing or conversion. See *United States v. Morissette*, 342 U.S. 246, 271 (1952) ("What has concerned codifiers of the larceny-type offense is that gaps or crevices have separated particular crimes of this general class and guilty men have escaped through the breaches. . . . The codifiers wanted to reach all such instances."). The Defense further argues that *Marshall* sets forth a precedent for a fatal variance. See Defense 641 Motion ¶¶ 27-30. In *Marshall*, the identity of the accused's custodian as charged was not proven. See *Marshall*, 67 M.J. at 420-21. Accordingly, the substitution of a different custodian changed the identity of the offense. *Id.* In this case, however, the identity of the records remains the same because the evidence relates to the charged databases and records. Thus, *Marshall* is not pertinent.<sup>3</sup>

Here, to "steal" means to wrongfully take money or property belonging to the United States Government with the intent to deprive the owner of the use and benefit temporarily or permanently. AE CDX. A conversion may include the misuse or abuse of United States property and may reach use in an unauthorized manner or to an unauthorized extent of property. *Id.* The misuse must seriously and substantially interfere with the United States Government's property rights. *Id.*

##### 1. Accused's acts constitute theft of United States Government Records

Theft of records occurs where copies of the records are transmitted to an unauthorized party even though the records remain in the custody and control of the United States. *United States v. DiGilio*, 538 F.2d 972, 977 (2d Cir. 1976). A copy of a record does not alter its character as a record under the ambit of § 641. *Id.* ("A duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen.") (citations omitted). Furthermore, the accused remains criminally liable under § 641 even where the United States retains possession of the original records. See *id.* (rejecting the accused's argument that § 641 does not apply where the United States, at most, loses exclusive possession of information contained in confidential records); see also *Flores-Figueroa v. United States*, 556 U.S. 646, 647 (2009) (upholding criminal liability for knowing transfer, possession, or use, without lawful authority, a means of identifying another person). Indeed, § 641 makes criminal the asportation of records owned by the United States. *DiGilio*, 538 F.2d at 977.

In his chat logs, the accused admitted to asporting the data from a United States Government computer system onto his personal computer and compromising the data by conveying it to Mr. Julian Assange. The accused stated, "[L]et's just say \*someone\* I know

<sup>3</sup> Changing the identity of the custodian prevents the accused from confronting the custodian. Here, the accused has been able to confront the custodians of the charged databases and records.

intimately well, has been penetrating US classified networks, mining data like the ones described . . . and has been transferring that data from the classified network over the "air gap" onto a commercial network computer . . . sorting the data, compressing it, encrypting it, and uploading it to a crazy white haired aussie who can't seem to stay in one country very long =L." PE 30 at 8 (ellipses in original). The accused admitted to compromising CIDNE-Iraq, CIDNE-Afganistan, and NCD. *Id.* at 8. The accused also admitted to compromising the USSOUTHCOM database, stating that Mr. Assange has "the 'Gitmo Papers.'" *Id.* at 46. The accused's admission provides a reasonable inference of his intent to deprive the United States Government permanently of the records and information contained therein.

Additionally, these statements corroborate the accused's intent to steal the USF-I GAL. The accused removed the USF-I from a United States Government computer system. CW4 Nixon testified that the only United States Government personnel had access to the USF-I GAL on NIPR system. The accused extracted the USF-I GAL from the United States Government system to his personal computer. This act constituted stealing. Moreover, the accused removed the USF-I GAL from the possession of the United States Government and placed it in his private possession after WikiLeaks posted a tweet specifically requesting military email addresses. *See* PE 31. The accused had the ability to view the USF-I GAL but did not possess the capability to export the USF-I GAL. *See* Testimony of CW4 Nixon. The accused searched for a macro, which is a computer program, that removed the USF-I GAL from a United States Government system. *See* PE 143. The accused also created a tasker to "exfiltrate" the USF-I GAL. *See* Testimony of Mr. Johnson; PE 122. Thus, the theft was complete the moment the accused took the USF-I GAL from the possession of the United States Government into his personal possession with the intent to deprive the United States of the stolen property. *See* AE CDX.

After-the-fact deletion of the record does not render innocent an already completed criminal act. The Defense's proffered argument regarding contradictory evidence is not appropriate under RCM 917. *See* 917(a) (stating that Defense may offer evidence if its request for a finding of not guilty is denied). Similarly, any evidence of transmission would only enhance the criminality of the already completed theft, but the lack of enhancement also does not render innocent a completed criminal act.

## *2. Accused's acts constitute conversion of United States Government records*

The existence of a property in the contents of confidential information has long been judicially recognized. *See Carpenter v. United States*, 484 U.S. 19, 25 (1987) (recognizing as worthy of protection a property right in confidential business information); *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979) (recognizing a property right in unpublished writings) (citations omitted). The United States Government is responsible for the accountability and dissemination of classified information and has set up certain procedures and precautions to protect classified documents and the information contained therein. *United States v. Zettl*, 889 F.2d 51, 53. The United States Government has created the systems for protecting classified information to protect its rights to confidentiality and exclusivity in the information it elects to classify. *See id.* (holding that authority to determine whether a document should be transferred is a function of the United States Government, not the holder of the document). Accordingly, the United States has a property interest in its classified records which it may protect by statute as a

thing of value under § 641. See *Girard*, 601 F.2d at 71. (citing *United States v. Friedman*, 445 F.2d 1076, 1087 (9th Cir. 1971). Conversion of computerized records as a “misuse or abuse of property its use in an unauthorized manner” occurs where an accused transfers information to an unauthorized party. See *id.* (holding that sale of information contained in computerized Drug Enforcement Agency records could be found to violate § 641 as a conversion of the computerized records) (citation and quotation marks omitted).

Conveyance of United States Government records to an unauthorized party constitutes conversion under § 641. See *DiGilio*, 538 F.2d at 976. In *DiGilio*, the defendants created unauthorized copies documents related to an investigation of alleged criminal activity and delivered the copies to unauthorized persons. *DiGilio*, 538 F.2d at 976. Based on these acts, the defendants were charged with converting to their own use “records of the United States; that is, photocopies of official files of the Federal Bureau of Investigation . . .” *DiGilio*, 538 F.2d at 976. Here, the accused converted the United States Government records by conveying them to WikiLeaks. WikiLeaks lacked the authority to possess this information. See Testimony of SA Mander; Testimony of Ms. Glenn; Testimony of Mr. Hosburgh. Defense’s reliance on *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995), is inapposite because *Collins* involved an infringement on computer systems within the possession on the United States Government and not the United States Government’s proprietary interest in its United States Government information. In the instant case, the accused stole and converted United States Government records by transferring them to an unauthorized party or onto his personal computer. Additionally, this conveyance harmed the United State’s interest in exclusive possession of the information in the records, thereby further adding to the conversion caused by the accused.

Furthermore, disclosure of United States Government proprietary information creates criminal liability for converting that information. See *Carpenter*, 484 U.S. at 26-27; *United States v. Fowler*, 932 F.2d 306, 309-10 (4th Cir. 1991). Specifically, misappropriating information confidentially held by one party by giving it to an unauthorized party constituted interference with the right to exclusive use of the compromised information. See *id.* In *Carpenter*, the author of an investment column entered into an agreement to give his co-conspirators advance information as to the content and timing of the article. *Id.* at 23. The contents of the articles were not affected and the owner of the information did not suffer a monetary loss. *Id.* at 23, 26. Nevertheless, the defendants’ conviction for wire and mail fraud under 18 U.S.C. § 1341 and 18 U.S.C. § 1343, each of which carried a potential sentence of up to five years, was upheld. See *id.* at 22 nn. 3-4. Deprivation of the right to exclusive use of the information established a sufficient basis for criminal liability because exclusivity was an important aspect of the confidential information. Accord *DiGilio*, 538 F.3d at 978 (finding merit to the Government’s argument that a misappropriation of information under § 641 but declining to so hold where a technical larceny was proven).

Here, the accused compromised classified, other United States Government information, or PII. This information had value because it was closely held. See Testimony of Mr. Lewis. The United States Government classifies information, *inter alia*, to protect it from adversaries. See *id.* Adversaries seek United States Government information to attack the United States. See PE 183. Thus, the accused substantially interfered with United States Government information by compromising it to WikiLeaks.

## B. Copies Do Not Constitute a Material or Prejudicial Variance

The Defense asserts a fatal variance on two bases. First, the Defense states that the distinction between “information,” “database,” and “copy” affects valuation and any preparation for the valuation element of the § 641 specification. Defense 641 Motion ¶ 26. As discussed in Part III, *infra*, this Defense argument ignores established precedent for determining valuation. Second, the Defense maintains that the distinction between stealing a “database,” “information,” or “copies of records” alters the substance of the § 641 specification and harms the accused’s ability to present a defense to the § 641 specifications. Defense 641 Motion ¶ 30.

The accused stole and converted records maintained on United States Government computer systems. The Defense argues that a fatal variance exists because the Charge Sheet specifies records and not copies of records. See Defense 641 Motion ¶ 4. The records compromised by the accused are the records maintained by the United States. The United States maintained copies of the records because they were digitally stored on United States Government computer systems. In this case, any distinction between copies of the records is feeckless because the records were stored digitally. See *DiGilio*, 538 F.2d at 978 (referring to theft of copies as “an asportation of records owned by the United States”) (emphasis added). This distinction cannot be a material variance because it does not change the nature of the offense, let alone substantially change the nature of the offense, increase the seriousness of the offense, or the punishment of the offense. Thus, any variance is not material.

Moreover, any variance between a digital record and a digital copy of the same record is not prejudicial. The distinction does not place the accused at risk of another prosecution because the accused is charged with stealing and converting the actual records, which he in fact stole and converted. Nor did the distinction affect the accused’s ability to prepare his defense because the United States charged the accused with stealing and converting the records using a term, “database,” the accused himself used to describe the records he compromised.

## C. No Variance Regarding USF-I GAL

The United States admitted evidence that the accused stole the USF-I GAL, and the Defense allegation that the property stolen by the accused was not, in fact, the USF-I GAL lacks merit. CW4 Nixon testified that the USF-I GAL had approximately 160,000 users. See Testimony of CW4 Nixon. CW4 Nixon testified that the USF-I GAL contained, *inter alia*, names and email addresses connected to the “iraq.centcom.mil” domain. *Id.* CW4 Nixon further testified that he identified names in PE 47 he personally knew existed in the USF-I GAL and that the “iraq.centcom.mil” domain was associated with the names, to include GEN Odierno and then-LTG Austin in PE 47. *Id.* CW4 Nixon testified that the USF-I GAL was distributed by organization, to include by division at the division level. See *id.* CW4 Nixon testified that the domain control of USF-I GAL at the division level established distributional control of the USF-I GAL. See *id.* CW4 Nixon testified that the USF-I GAL was also distributed at the Corps and brigade levels. See *id.* CW4 Nixon testified that PE 47 and PE 48 constituted a USF-I GAL pool for a USF-I server. *Id.* CW4 Nixon identified the contents of PE 47 and PE 48 as reflecting the contents of the USF-I GAL. CW4 Nixon also testified that PE 147 and PE 148 were representative of the contents of PE 47 and PE 48, respectively.

CW4 Nixon testified that a user would not have the ability to download the USF-I GAL or its subordinate portions without a special program or access privileges. *See id.* CW4 Nixon testified that downloading the USF-I GAL as a whole or in part was not a function. CW4 Nixon distinguished between a user being able to view the entire USF-I GAL and accessing the USF-I GAL; accessing the USF-I GAL entailed the ability to remove the USF-I GAL from the United States Government systems. CW4 Nixon testified that a user could cut and paste the information from the USF-I GAL but that such a process would not be effective. *See id.* CW4 Nixon also testified that removing the contents of the USF-I GAL would not be easy without outside software or programming. *See id.* SA Williamson testified that he found the contents of a Microsoft GAL on the accused's computer. *See* PE 143. SA Williamson also testified that the accused searched for a macro to export a GAL. *See* PE 143. Also, the accused created a tasker to "exfiltrate" the USF-I GAL. *See* Testimony of Mr. Johnson; PE 122.

Assuming, *arguendo*, that the United States has not adduced evidence that the accused stole the entire USF-I GAL but only a large portion of it, no fatal variance exists for Specification 16 of Charge II. Any such variance is minor because it does not change the nature of the offense. *See United States v. Lovett*, 59 M.J. 230, 235-36 (C.A.A.F. 2004) (citations omitted). At a minimum, the evidence establishes that the accused stole the USF-I GAL as distributed at the division level. *See* Testimony of CW4 Nixon.

The Defense was fully aware of the United States Government property at issue. Furthermore, the admitted evidence constitutes at least part of the USF-I GAL as charged in Specification 16 of Charge II. Evidence that a portion of the charged property was stolen does not constitute a fatal variance. *See United States v. Kubel*, 5 C.M.R. 73, 75-76 (C.M.A. 1952) (upholding substitutions and exceptions that reduced the number and value of stolen items); *United States v. Lee*, 1 M.J. 15, 16-17 (C.M.A. 1975) (holding defense counsel was not misled where the Government submitted evidence that marijuana plants were part of the quantities covered in the specification); *England v. United States*, 174 F.2d 466, 468 (5th Cir. 1949) (holding no fatal variance between "check" and "an incompleted draft on the Treasurer of the United States"); *see also United States v. Thomas*, 65 M.J. 132, 135-36 (amending specification to change a specifically charged quantity to "some quantity"). The Defense contends that *United States v. Wilkins*, 45 C.M.R. 638 (A.C.M.R. 1972), demonstrates that the alleged variance is fatal. However, *Wilkins* held that a variance is fatal where it completely changes the stolen *res* from an amount of currency to a wallet. *See Wilkins*, 45 C.M.R. at 639-40. Here, the accused is charged with stealing the USF-I GAL and its contents, and the evidence demonstrates, at a minimum, that a large portion of the contents of the USF-I GAL were stolen. Thus, any variance regarding the amount of the USF-I GAL that was stolen is not fatal.

### III. VALUATION IS PROVEN BY INFORMATION

#### A. Information Is Intrinsic to Compromised Records

Defense claims about prejudice stemming from valuation disregard the methods of proving valuation. Under § 641, valuation may be demonstrated by face value, par value, market value, or cost price. § 641. § 641 protects "a thing of value." *Id.* A thing of value includes



tangible and intangible items. See *Fowler*, 932 F.2d 306, 309-310 (4th Cir. 1991) (determining that records and the information contained in the records qualify as a thing of value under § 641) (citing *Carpenter*, 484 U.S. at 25; *Morison*, 844 F.2d at 1076-77). Information is an intangible thing of value protected by § 641. See *id.*; cf. *United States v. Schwartz*, 785 F.2d 673 (9th Cir. 1986) (interpreting “thing of value” under § 641 to “include . . . intangibles, such as providing assistance in arranging the merger”); *United States v. Croft*, 750 F.2d 1354, 1362 (7th Cir. 1984) (holding that § 641 applies to research services as a thing of value); *Burnette v. United States*, 222 F.2d 426 (6th Cir. 1955) (holding services and labor performed by government employees are punishable under § 641). Indeed, proprietary information in United States Government records is a thing of value under § 641. See *Fowler*, 932 F.2d at 310 (noting that information is a species of property and a thing of value); *United States v. Jeter*, 775 F.2d 670, 680-82 (6th Cir. 1985); *Girard*, 601 F.2d at 70-71.

Valuation for a § 641 specification may be demonstrated, *inter alia*, by the item’s market value, thieves’ market value, or cost of production. Market value is “approximately what it would cost to purchase the same or similar property in the marketplace.” *United States v. 50 Acres of Land*, 469 U.S. 24 (1984); see *Muser v. Magone*, 155 U.S. 240 (1894) (defining market value as the “price at which the owner of the goods, or the producer, holds them for sale; the price at which they are freely offered in the market to all the world; such prices as dealers in the goods are willing to receive, and purchasers are made to pay, when the goods are bought and sold in the ordinary course of trade”). The thieves’ market value is the price at which the good may be sold on the illegal black market. See, e.g., *United States v. Hood*, 12 M.J. 890, 891-92 (A.C.M.R. 1982); see also *United States v. Ligon*, 440 F.3d 1182 (9th Cir. 2006) (defining the market value approach to include the thieves’ market). The cost of production is the price the producer incurred to create or produce the good. See, e.g., *United States v. Walter*, 43 M.J. 879, 885 (N-M. Ct. Crim. App. 1996). The cost of production has been applied to calculate the value of deleted database files for which “no readily ascertainable market value” existed. *Id.*

Additionally, the cost of production includes costs producing and supporting the use of the records. See *Zettl*, 889 F.2d at 54 (noting that cost price includes the cost of photocopying, transportation, and other actual costs of the documents); *Walter*, 43 M.J. at 884-85 (deciding that the personnel or labor costs of producing and reproducing the files was reasonable). The Defense relies on *Zettl* to argue that the scope of valuation should be narrowed. See Defense 641 Motion ¶ 44. However, the accused is charged with stealing or converting databases, to include the records contained therein, and not documents as charged in *Zettl*. See Charge Sheet; *Zettl*, *supra*. Given the infrastructure necessary to support the databases and the records contained therein, the costs of producing and maintaining the databases are relevant under § 641. See, e.g., PE 115; PE 116; PE 131; Testimony of CW4 Nixon; Testimony of Mr. Wisecarver.

The basis of establishing a market value, to include the thieves market, requires an analysis of the characteristics of the actual goods. See, e.g., *Hood*, 12 M.J. at 891-92 (comparing values of stolen goods to values received on black market of similar goods). The market value is determined by the value the participants place on the record, to include its information. See *Ligon*, 440 F.3d at 1184 (“[P]roperty value is determined by market forces . . . . This gives § 641 its obvious, and certainly its practical, meaning, namely the amount the goods may bring to the thief.”).



The contents of the record dictate its value. *See* Testimony of Mr. Lewis. No open market for United States Government information exists. *See id.* Further, bulk amounts of information have increased value in comparison to smaller collections of records. *See id.* Where valuation can be proven by the value of the goods in a market, evidence that the records are valuable to adversaries based on their contents does not prejudice the accused. *See United States v. May*, 625 F.2d, 186, 191-92 (6th Cir. 1980) (deciding that a determination of a thing of value can rely on the readily ascertainable and quantifiably components of the stolen or converted thing of value). Similarly, evidence of the cost of production for the databases and records contained therein cannot be separated from the information because the information requires protection. *See, e.g.*, Testimony of Mr. Lewis; *May, supra*. The Defense attacks Mr. Lewis's credibility, but the Defense Motions are not the appropriate forum for argument regarding witness credibility. *See* RCM 917(d). Thus, evidence of value of the records, to include their information, poses no prejudice to the accused.

#### B. Defense Has Had Ample Notice of Valuation Based on Information

The appellate record demonstrates that the Defense has been on notice that the United States intended to elicit testimony from Mr. Lewis on the value of government information since well before the start of this trial, and specifically that the United States intended to offer him as an expert in this field. Below are excerpts from both the United States and Defense filings that outline this notice:

On 26 October 2012, the United States stated in its witness list #2 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CCCLXVII at 8.

On 12 December 2012, the United States stated in its witness list #3 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDXXXVI; AE CDXXXVIII at 8.

On 31 January 2013, the United States stated in its witness list #4 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXV; AE CDLXXVI at 7.

On 31 January 2013, the United States stated in its Grunden response that Mr. Lewis "will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXIX; AE DLXXX at 18.

On 1 February 2013, the United States stated in its Grunden response corrected copy that Mr. Lewis "will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXIX; AE DLXXX at 18.

On 22 February 2013, the Defense stated in its MRE 505(h) notice that Mr. Lewis "is a counterintelligence specialist with DIA and has worked in the field generally for many years." AE CDXC at 14. The Defense explains that the United States provided the following as an explanation of his testimony- "He will testify about counterintelligence and the value of information, including classified information concerning the value of government information." *Id.* The defense further states:

The matters covered by the defense in cross examination will fall within the general outlines provided by the Government above. The defense reasonably expects to discuss the experience of Mr. Lewis on other cases. That experience gives Mr. Lewis the expertise to opine as to the value of government information.

*Id.*

On 24 April 2013, the Defense stated in its Grunden filing that Mr. Lewis will testify about the "value of CIDNE [d]atabases, charged SOUTHCOM information, and the USF-I GAL." AE CXXVat 16. In the same filing, they also stated Mr. Lewis will "testify about how the value of those items and how their value is determined." *Id.* Additionally, the Defense stated that he will testify about money offered for the information in the databases and "generally about how the information, even if dated, will be of some value" to foreign entities. *Id.*

On 10 May 2013, the United States filed its notice of accounting of discovery and expert witnesses, which stated next to Mr. Lewis's name that "[t]he United States may qualify this witness as an expert in counterintelligence and the value of national security information[.]" AE CXLIII at 4.

On 13 May 2013, the Defense stated in its corrected copy of its Grunden filing that Mr. Lewis will testify about the "value of CIDNE [d]atabases, charged SOUTHCOM information, and the USF-I GAL." AE CXV at 16. In the same filing, they also stated Mr. Lewis will "testify about how the value of those items and how their value is determined." *Id.* Additionally, the Defense stated that he will testify about money offered for the information in the databases and "generally about how the information, even if dated, will be of some value" to foreign entities. *Id.*

On 15 May 2013, the United States filed a corrected copy of its notice of accounting of discovery and expert witnesses, which stated next to Mr. Lewis's name, "The United States may qualify this witness as an expert in counterintelligence and the value of national security information[.]" AE CLXIII at 4.

Thus, the Defense has had ample notice about the United States' intention to rely on the information contained in the compromised records to establish valuation. Therefore, the Defense has not suffered any prejudice.

### CONCLUSION

The United States submitted evidence relevant to the § 641 specifications that was admitted. The Defense argues that the United States has failed to satisfy the standard set forth in RCM 917(d). The admitted evidence establishes a reasonable inference that the accused stole and converted the databases and records listed in the § 641 specifications. The Defense arguments that the § 641 specifications constitute fatal variances lack merit because the evidence proves the contents of the databases and the records were stolen or converted. The evidence does not constitute a material variance. Additionally, the Defense had adequate notice and ability to prepare the accused's defense for trial.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 11 July 2013.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Response

to Defense Motion for  
Directed Verdict: Article 104

11 July 2013

### RELIEF SOUGHT

The prosecution in the above case respectfully requests the Court deny the defense request to enter a finding of not guilty as to the Specification of Charge I (pursuant to Rule for Courts-Martial (RCM) 917(a)).

### BURDEN OF PERSUASION AND BURDEN OF PROOF

A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense most favorable to the prosecution, with an evaluation of the credibility of witnesses. RCM 917(d).

### FACTS

The prosecution began its case in chief on 3 June 2013 and rested on 2 July 2013. The defense filed its motions for directed verdict on 4 July 2013.

### WITNESSES/EVIDENCE

PE 1: OMPF

PE 5: 35F Program of Instruction and Lesson Plan

PE 6: 35F AIT Student Evaluation Plan

PE 11: Hard drive - DN #073-10 Item 1 - Classified (Accused's External Hard Drive)

PE 12: Hard drive - DN #073-10 Item 1 - Classified (.22)

PE 25: Powerpoint "Operations Security" dtd 13 Jun 08

PE 30: Wired.com chat logs (Manning/Lano)

PE 35: Stipulation of Expected Testimony, Elisa Ivory, 10 May 13

PE 36: Stipulation of Expected Testimony, SSG Alejandro Marin, 30 May 13

PE 42: Readme.txt

PE 43: Chaos Communication Congress report by SSG Matthew Hosburgh, dtd 7 Jan 2010 (declassified)

PE 45: ACIC Special Report, Wikileaks.org-an Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups? (unclassified w/out references)

PE 51: Power Point slides "Issue: Islamic Extremism"

PE 52: Power Point slides "Information Security AR 380-5" from 305th MI Battalion

PE 58: Email from Manning to Ehresman and Hack, dtd 12 Jan 10 - Classified  
PE 59: Manning Non-Disclosure Agreement witnesses by Rubin (aka Ivory), dtd 7 Apr 08  
PE 60: Manning Non-Disclosure Agreement witnessed by Balonek, dtd 17 Sep 08  
PE 61: CD Containing Intelink Logs for .22 and .40 - Classified  
PE 63: ACIC Website Logs  
PE 64: ACIC Webserver Logs  
PE 70: Stipulation of Expected Testimony, Mr. Peter Artale  
PE 85: Intelink Log Summary (C3 and NCIS Documents)  
PE 99: NCIS IIR  
PE 120: Buddy List from PFC Manning's Personal Mac Listing Press Association Contact Information  
PE 123: Chats recovered from PFC Manning's Personal Mac between Press Association and dawgnetwork  
PE 127: Volumes.txt  
AE 81: Court Ruling, Def Motion Dismiss The Sp of Ch I, FTSAO, 26 Apr 12  
AE 410: Court's Draft Instructions  
DE J: Report of Examination of PFC Manning's Personal Laptop Classified  
Testimony of CPT Fulton  
Testimony of CW2 Balonek  
Testimony of CW2 Hack  
Testimony of Mr. Hosburgh  
Testimony of Mr. Johnson  
Testimony of Mr. Madrid  
Testimony of Mr. Moul  
Testimony of SA Mander  
Testimony of SA Shaver  
Testimony of SA Smith  
Testimony of SFC Anica

### LEGAL AUTHORITY AND ARGUMENT

The sole allegation in the defense's motion with regard to Article 104 is that the prosecution did not present evidence that the accused had "actual knowledge" that by giving information to WikiLeaks, he was giving information to an enemy of the United States. Defense RCM 917 Motion for Article 104 at 1.

Only "some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged" is necessary to withstand a motion for a directed verdict. RCM 917(c). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*; see also *United States v. Perez*, 40 M.J. 373 (C.M.A. 1994) (upholding the military judge's decision not to enter a finding of not guilty because the testimony of three witnesses, construed in the light most favorable to the prosecution, could reasonably tend to establish the overt act). Courts agree the "some evidence" standard to survive a motion for a finding of not guilty is a low one. See *United States v. Escochea-Sanchez*, 2013 WL 561356 (N-M.Ct.Crim.App. 2013) (concurring with the military judge who "noted repeatedly while hearing

argument on the RCM 917 motion [that] the standard for surviving such a motion is very low"); *see also United States v. Jenkins*, 59 M.J. 893, 898 (A.C.C.A. 2004) (encouraging trial judges to view the standard used to decide whether to grant a motion for a finding of guilty as a mirror image of the standard used to decide whether to give an instruction on an affirmative defense); *United States v. Athearn*, 1994 WL 711894 (A-F.Ct.Crim.App. 1994) (quoting RCM 917(d)) (noting that "[t]he military judge was obviously correct in denying the motion for a finding of not guilty under the low, 'some evidence' standard set out in RCM 917(d)").

According to the Court's draft instructions for the Specification of Charge I,

"knowingly" requires actual knowledge by the accused that by giving the intelligence to the 3rd party or intermediary or in some other indirect way, that he was actually giving intelligence to the enemy through this indirect means. This offense requires that the accused had a general evil intent in that the accused had to know he was dealing, directly or indirectly, with an enemy of the United States. 'Knowingly' means to act voluntarily or deliberately. A person cannot violate Article 104 by committing an act inadvertently, accidentally, or negligently that has the effect of aiding the enemy.

Appellate Exhibit (AE) 410 at 2; *see also United States v. Batchelor*, 22 C.M.R. 44 (C.M.A. 1956). The explanation of "Knowledge" in Article 104(c)(5)(c) for "Giving intelligence to the enemy" also states that "Actual knowledge is required but may be proved by circumstantial evidence." Article 104(c)(5)(c), Uniform Code of Military Justice (UCMJ). This definition is quoted in "The Law: Article 104" portion of the Court's Ruling on the Defense Motion to Dismiss for Failure to State an Offense. AE 81; *see also RCM 918(c)* (Findings may be based on direct or circumstantial evidence.). "There is no general rule for determining or comparing the weight to be given to direct or circumstantial evidence." RCM 918(c), discussion. Direct or circumstantial evidence satisfies the "some evidence" standard. *See United States v. Parker*, 59 M.J. 195 (C.A.A.F. 2003); *United States v. Varkonyi*, 645 F.2d 453, 458 (5th Cir. 1981). Although not explicitly enumerated in the draft instruction of "knowingly" for Article 104, in the draft instruction for "knowledge" in Specification I of Charge II the Court specifically notes that, "Knowledge, like any other fact, may be proved by circumstantial evidence, including the accused's training, experience, and military occupational specialty." AE 410 at 3.

The prosecution elicited a plethora of evidence in its case in chief to prove that the accused had the requisite knowledge for the Specification of Charge I. The evidence that the prosecution presented to establish the accused's actual knowledge can be broadly defined under three categories: (1) Military education and training; (2) information the accused reviewed during the course of his misconduct; and (3) statements by the accused.

#### 1. Military Education and Training

The defense acknowledged that the prosecution introduced evidence that, in his training, the accused was instructed that the enemy uses the internet generally. *See Defense RCM 917 Motion at 2.* The defense, however, argues that the prosecution has not proffered any evidence

that shows that the accused was instructed that a particular enemy looks at or uses the WikiLeaks website.

The prosecution notes a factual inaccuracy in paragraph 5 of the defense's argument. In response to the defense in cross-examination, Mr. Johnson testified he did not look at or recover any websites that were associated with terrorism or with a hatred of America or anti-American beliefs in his forensic examination of the accused's personal Macintosh computer, rather than what the defense proffered. Testimony of Mr. Mark Johnson. Mr. Mark Johnson did not say "that his forensic investigation of PFC Manning's computer revealed no searches for the enemy, anything related to terrorism, or anything remotely anti-American." Defense RCM 917 Motion for Article 104 at 2.

a. AIT Training

The prosecution established in its case-in-chief that the accused is an all-source intelligence analyst (35F). *See, e.g.*, Prosecution Exhibit (PE) 1 (OMPF).

The prosecution presented evidence that during AIT, the accused committed an operational security (OPSEC) violation and, as part of corrective training, was specifically required to research and brief the importance of OPSEC and the potential damage or harm to national security by having an OPSEC violation. *See* Testimony of Mr. Madrid. The accused presented three different types of corrective training (a brief, a Power Point, and a written report) that covered the importance of OPSEC. *See* Testimony of Mr. Madrid; PE 25 (Power Point presented by the accused on OPSEC). The accused's Power Point was found on his external hard drive, which was recovered from the Accused's CHU in Iraq. *See* Testimony of SA Smith; Testimony of Mr. Johnson; DE J. In his Power Point, the accused noted that, among others, adversaries included foreign governments, terrorists, activists, and hackers. Testimony of Mr. Madrid; PE 25 (Power Point presented by the accused on OPSEC). In his Power Point, the accused also documented "Common OPSEC Leaks" which included the Internet and concluded that disclosure of information, including posting on the Internet, must be avoided and that one must use common sense because there are many enemies and it is a free and open society. *Id.*

The prosecution also presented evidence on the accused's training as an all-source intelligence analyst and that training included training on the identities of terrorist groups, which included Al-Qaeda. *See* Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan); PE 51 (Power Point slides on the enemy). The prosecution also presented evidence that the accused was trained that the enemy used the internet and that anything that the enemy can use or piece together to use against the United States should be protected, in include, among other things, PII and unit identification and movement information. *See* Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan); PE 51 (Power Point slides on the enemy); PE 52 (Power Point slides from AIT on INFOSEC); PE 36 (Stipulation of Expected Testimony, SSG Marin); PE 35 (Stipulation of Expected Testimony, Ms. Ivory). For example, slide 71, which is supplemented by the text in the corresponding 35F AIT lesson plan, and was taught to the accused by Mr. Moul states, "The enemy will attempt to discover how and when we are conducting operations, knowing this, we must protect our activities from detection. We do this

by: •Identifying - Critical Information •Analyzing - Threat." See PE 52 (Power Point slides from AIT on INFOSEC); Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan). Slide 72 defines "Critical Information" as, among other things, installation maps with highlights of designated points of interest, SOPs, TTPs, unit capabilities and intent, and personal/family information. *Id.* Slide 73, entitled "Prevent Disclosures" says "DON'T DISCUSS OPERATIONAL ACTIVITIES ON THE WEB". *Id.* Training slide 73 that the accused received at AIT goes on to say, "Ensure information posted has no significant value to the adversary"; "Always assume the adversary is reading your material"; and "Remember it is called the World Wide Web for a reason." *Id.* The accused also received training on the different types of recruiting utilized by terrorist organizations, particularly by Al-Qaeda, and that the number of terrorist websites have jumped from less than 100 to as many as 4,000 in the last ten years and many insurgency groups have many sites and message boards to help their network. Testimony of Mr. Moul; PE 51 (Power Point slides on the enemy and their use of the Internet). The accused had to pass a test on INFOSEC/OPSEC in order to proceed in the course. See Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan).

The training demonstrates that the accused knew who the enemy was and that the enemy used the internet. The accused passing a test on INFOSEC/OPSEC and his corrective training further demonstrate that he was not only taught the information, but he learned it and had an appreciation for its importance. A reasonable inference follows that since Wikileaks.org is a website on the Internet, and the accused knew that the enemy was looking for any and all information on the Internet, that the Accused knew that by putting information on the Internet, he was giving the information to the enemy. This is particularly true in light of the information that the accused was giving to Wikileaks.org, which he was specifically trained was of interest to the enemy. The accused's knowledge of enemy receipt is an inevitable conclusion given the evidence the prosecution presented on the accused's knowledge of the type of website that Wikileaks.org was at the time the accused unlawfully transmitted the information to them (discussed below). This is circumstantial evidence of the accused's actual knowledge.

#### b. Non-Disclosure Agreements

In addition, the prosecution offered evidence that the accused had to sign non-disclosure agreements (SF 312). See Testimony of Mr. Moul; PE 35 (Stipulation of Expected Testimony, Ms. Ivory); PE 59 (Accused NDA, dtd 7 Apr 08); Testimony of CW2 Balonek; PE 60 (Accused NDA, dtd 17 Sep 08). The non-disclosure agreements described the responsibilities and special trust and confidence associated with having access to classified information. See PE 59 (accused NDA, dtd 7 Apr 08); PE 60 (accused NDA, dtd 17 Sep 08). The non-disclosure agreements explain the potential damage and consequences associated with the unauthorized disclosure of that information. *Id.* Furthermore, the non-disclosure agreements highlights that the classified information was the property of the US government. *Id.* The significance of the NDA was also explained to the accused. Testimony of Mr. Moul; PE 35 (Stipulation of Expected Testimony, Ms. Ivory); Testimony of CW2 Balonek. The accused even raised his right hand and vowed to uphold the responsibilities contained in the non-disclosure agreement. See PE 35 (Stipulation of Expected Testimony, Ms. Ivory). Understanding and signing the non-disclosure agreements further ensured that the accused understood the importance of protecting classified information



and the consequences of its unauthorized release. This is circumstantial evidence of the accused's actual knowledge.

c. Additional Information on the Accused's External Hard Drive

The prosecution admitted the accused's external hard drive. See PE 11. That external hard drive contains a wealth of training information in addition to the accused's OPSEC slideshow discussed above. *Id.* Specifically, it contained the following:

- the accused had a Microsoft PowerPoint brief titled "Insurgent Propaganda TTPs" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\Lessons Learned\Lessons Learned\Threat\UFOUO\_Iraqi\_Propaganda\_TTPs\_Brief\_26Jan05.ppt).<sup>1</sup> Slide 17 says "Insurgent Information operations (IO) becoming increasingly sophisticated – videos on the internet and favorable news coverage on Arab media Al Jazeera (see list of pro-insurgent websites)." *Id.*

- the accused had a copy of FM 2-0 titled "Intelligence" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Field Manuals\FM\_2\_0-intel.pdf). The document states adversaries "weaponry may range from a computer connected to the Internet to WMD." *Id.*

- the accused had a copy of AR 525-13 titled "Antiterrorism" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\O&NOIP\SOP's\_AR's\AR525\_13 Anti-Terrorism.pdf). It states that terrorists use "instances of web site tampering to further their cause." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\fm7\_100x1.pdf). This document states "Rapid advances in technology have produced an incredibly complex global information environment. Information and communications technologies have grown exponentially in recent years. Satellite and cellular communications, direct-broadcast television (expanding the awareness of events, issues, and military activities), personal computers, global positioning system (GPS) technologies, wireless communication capabilities, and the Internet are a few examples of the capabilities widely available to nations, as well as independent organizations and individuals. Given such advances, the capabilities of both the OPFOR and its potential adversaries are increasing in both sophistication and lethality. The OPFOR tries to exploit such technologies to gain the operational advantage." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\fm7\_100x1.pdf). This document

<sup>1</sup> PE 11 and PE 12 are compilation exhibits that were admitted and contain computer images of the accused's external hard drive (PE 11) and "22" SIPRNET computer (PE 12). The prosecution can provide the Court with the appropriate viewing equipment or can print each item referenced within this motion for the Court.

states "In contrast to other forms of warfare, IW [(Information Warfare)] actions might occur without access to large financial resources or backing or without state sponsorship. Information weapons could be software logic bombs or computer worms and viruses. IW could be conducted with such easily accessible means such as cellular telephones and the Internet." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-1.pdf). Chapter 5 of this document provides an overarching discussion of Information Warfare. *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states that "Depending on the size, nature, and focus of the insurgent organization, the direct action cell (IW) may be capable of several functions. Some example functions . . . [include assisting] . . . in the cyber-mining for intelligence. All of these functions are integrated to further short- and long-range goals." *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states "Close coordination is maintained with the IW cell for Internet communications." *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states "The internet is a powerful recruitment tool. The recruiting cell maintains close coordination with the information warfare cell." *Id.*

The accused's possession of all the above information is additional circumstantial evidence that the accused knew and understood all of the above information, leading to the reasonable inference that the accused knew that by disclosing information to WikiLeaks.org he was giving the information to the enemy, and specifically Al-Qaeda.

d. Accused Knowledge of SIGACTs

In addition to offering evidence on the type of information the accused would be seeking on the Internet, the prosecution also offered evidence that the accused was aware that SIGACTs included the type of information that the enemy would be seeking and that the accused knew that the SIGACTs were valuable and useful intelligence as discussed below. The accused acknowledged the value by stating in the text file that accompanied the disclosed CIDNE databases on the accused's SD Card stating, "This is possibly one of the more significant

documents of our time, removing the fog of war, and revealing the true nature of 21st century asymmetric warfare." PE 42 (Readme.txt); *see* Testimony of SA Shaver.

The prosecution offered numerous witnesses to testify regarding the accused's knowledge of SIGACTs. *See, e.g.*, Testimony of SFC Anica; Testimony of CW2 Hack; Testimony of CPT Fulton; Testimony of CW2 Balonek. According to SFC Anica, it was part of the accused's job, in garrison, to combine information from the SIGACTs and pick out the most relevant and important data and then create PowerPoint presentations to brief the S2; vehicle-borne IEDs were particularly significant at the time. Testimony of SFC Anica. According to CW2 Hack, the accused had many SIGACTs organized in his folder on his unit's share drive in an extremely meticulous manner. Testimony of CW2 Hack. The SIGACTs and other intelligence reports were organized by geographical locations that were tied to an enemy threat group that the leadership had prioritized. *Id.* The accused knew of the value and usefulness of SIGACT reports when conducting an analysis of unit activity, as he used the SIGACTs to create work product. *See id.*; PE 58. Specifically, the accused gave CW2 Hack a SIGACT report of an IED attack that had a unit in the same area of operation that 2d Brigade, 10th Mountain was in, two years before they arrived to assist CW2 Hack with his targeting mission as the Accused thought the SIGACT would be assist in the capture of a high value target. *Id.* The attack described the type of weapon system that was used, as well as damage and equipment that was used. *Id.* It also included an S2 assessment of the event. *Id.* Similarly, the accused pulled SIGACTs for CPT Fulton, which would typically focus on IEDs, small arms, and direct and indirect fire. Testimony of CPT Fulton. The accused would mine the information, organize the information, sort the information, and then plot the SIGACT information on the map, so it was represented visually and so analysis could be conducted based on enemy patterns and engagement areas represented. *Id.* The accused also pulled SIGACTs from CIDNE, and organized them on an excel spreadsheet to show enemy trends. *Id.* CPT Fulton also testified that, in garrison, the Accused helped her prepare the intelligence portion of the OPORD for the deployment. *Id.* Specifically, the accused gave CPT Fulton the basis of knowledge on all of the enemy threat groups. *Id.* Finally, according to CW2 Balonek, the accused put together an intelligence product that compared the past three years of Iraq SIGACTs, and specifically looked at locations of different types of attacks, such as IED attacks and small arms fire against convoys. Testimony of CW2 Balonek.

The evidence offered by the prosecution is a reasonable inference to show the accused knew the value of the SIGACTs from an intelligence point of view. He knew that individual SIGACTs could be used to create actionable intelligence products for the Commander. He also knew the value of having numerous SIGACTs and the products that could be created from the SIGACTs. He knew a group of SIGACTs could be used to decipher patterns of behavior of friendly and enemy units. Just as the accused would use SIGACTs to decipher enemy tactics, techniques, and procedures (TTPs), the accused knew that the enemy would find the same value in the ability to decipher our TTPs, and would find similar value in the ability to create actionable intelligence products from the SIGACTs. All the above leads to a reasonable inference that the accused knew of this value prior to disclosing the SIGACTs to Wikileaks.org to be posted on the internet, to be accessible to all people globally, including the enemy. The above also leads to a reasonable inference that the accused knew that this information was

exactly the type of information that the enemy would seek out and access and that the enemy would have access to all the information as leaked on Wikileaks.org.

## 2. Information Accused Accessed During the Course of his Misconduct

### a. ACIC Report

The defense acknowledged that the prosecution introduced evidence to show that the accused accessed the ACIC report titled "Wikileaks.org--An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" charged in Specification 15 of Charge II. *See* Defense RCM 917 Motion at 2. The defense, however, argues that accessing this article does not show that the accused had actual knowledge that by giving information to Wikileaks, he was giving it to the enemy. *Id.* The defense argues how the accused interpreted the report in their motion; however, there is no evidence of that interpretation by the accused. *Id.* These are the defense's interpretations and reserved for argument, thus not appropriate for a RCM 917 motion. RCM 917(c) requires the Court to view the evidence "in the light most favorable to the prosecution." RCM 917(c).

The purpose of the ACIC report, which was published on 18 March 2008, was to "assess the counterintelligence threat posed to the US Army by the Wikileaks.org Web site." PE 45 (Unclassified ACIC Report). The ACIC report describes in detail what the author's research of Wikileaks.org revealed about Wikileaks.org, their actions, and how they operated in 2008. *See* PE 45 (Unclassified ACIC Report). The first bulleted "Key Judgment" of the ACIC report is that "Wikileaks.org represents a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army." PE 45 (Unclassified ACIC Report). The second bullet states, "Recent unauthorized release of DoD sensitive and classified documents provide FISS, foreign terrorist groups, insurgents, and other foreign adversaries with potentially actionable information for targeting US forces." *Id.* The sixth bullet says that "Wikileaks.org most likely has other DoD sensitive and classified information in its possession and will continue to post the information to the Wikileaks.org Website." *Id.* The ACIC report goes on to discuss the DoD and classified information that Wikileaks.org has released in the past and how Wikileaks.org posts all information that they receive without editorial oversight. *Id.* The ACIC report concludes that "it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the WL.org web site" and warns of adversaries increased ability to complete rapid data compilation to more efficiently develop actionable information for their use for intelligence collection, planning, or targeting purposes. *Id.*

The prosecution also offered evidence that the accused searched for Wikileaks.org or variations of that term over 100 times between 1 December 2009 and 15 March 2010 on SIPRNET. Testimony of SA Shaver; PE 61 (Intelink logs). The logs further prove that he further supplemented his knowledge of Wikileaks.org through these searches. *Id.* The prosecution also admitted the image of the accused's .22 computer. *See* PE 12. That image contains an email that the accused sent to members of the S2 section (CPT Lim, CPT Martin, CW2 Ehresman, 1LT Gaab, CW2 Balonek, SPC Madaras, SPC Cooley) on 15 March 2010, classified FOUO. PE 12 (PFC MANNING Primary SIPR\2251-27May10\2251-27May10\CDocuments and Settings\bradley.manning\Local Settings\Application

Data\Microsoft\Outlook\archive.pst\Root folder\Top of Personal Folders\Deleted Items\Sent Items\1[UNCLASSIFIED//FOR OFFICIAL USE ONLY] ACIC Cyber Collaboration Portal [UNCLASSIFIED//FOR OFFICIAL USE ONLY]). In that email, the accused states, "Occasionally has good hits from extremist websites in our OE! Found it earlier this evening. <http://acicportal.north-inscom.army.smil.mil/cyber/default.aspx>". *Id.* According to the ACIC logs, the ACIC report (Product ID # RB08-0617) is available at the URL "<http://acicportal.north-inscom.army.smil.mil/cyber/default.aspx>" and the accused linked to the ACIC report through that URL. *See* PE 64 (ACIC Webserver logs); PE 45 (Unclassified ACIC Report).

The prosecution offered evidence that the accused accessed the website containing the ACIC report on 1 December 2009, 29 December 2009, 1 March 2010, and 7 March 2010. PE 70 (Stipulation of Expected Testimony, Mr. Artale); PE 63 (ACIC metrics for the ACIC report). The prosecution also offered evidence that the accused viewed the ACIC document on 14 February 2010 and 1 March 2010. Testimony of SA Shaver; PE 61 (Intelink logs).

The above evidence leads to a reasonable inference that based on the accused's repeated access to the report, he not only read the ACIC report charged in Specification 15 of Charge II but that he read it multiple times. This is circumstantial evidence that the accused was put on notice that by giving information to Wikileaks.org, the enemy would have access to and use the information. The accused was also put on notice by the ACIC report that Wikileaks.org was not a legitimate media organization, since, according to the report, Wikileaks.org posts all information they receive with no editorial oversight. PE 45 (Unclassified ACIC Report). It is a reasonable inference that given the accused's specific training on Al-Qaeda, he knew the enemy would be Al-Qaeda based on the time period of the misconduct and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet.

b. IIR 5 391 0014 08

Similarly, the prosecution offered evidence of the accused's knowledge through IIR 5 391 0014 08. The subject of this IIR was "Internet Web Postings of Classified and for Official Use Only Documents." PE 99 (IIR 5 391 0014 08). The IIR discussed Wikileaks.org, and according to the report, in December 2006, "Wikileaks.org was established to encourage the anonymous posting of sensitive government and corporate documents." PE 99 (IIR 5 391 0014 08); *see also* Testimony of SA Mark Mander. According to the IIR, "Wikileaks.org self-describes as (quote) an uncensorable Wikipedia for untraceable mass document leaking and analysis (unquote)." *Id.* According to the 2008 report, numerous classified and FOUO documents have been posted and continue to be available on Wikileaks.org and its mirror sites. *Id.*

The prosecution offered evidence that the accused searched for the IIR on 14 February 2010. *See* PE 85 (Intelink logs); Testimony of Mr. Mark Johnson. The prosecution also offered evidence that the accused moved a copy of the IIR to his personal Macintosh computer on 15 February 2010. *See* PE 127 (Volumes.txt which showed the IIR was on the accused's personal Macintosh computer).

The above evidence leads to a reasonable inference that the accused's accessing the individual IIR and moving it to his personal computer demonstrates that the accused read the

document. Again, by reading the IIR, the accused was put on notice that by giving information to Wikileaks.org, a site that was quickly gaining a reputation for encouraging leaks of classified government information and a website that seemingly posted everything it received, would be used by the enemy. This is circumstantial evidence that the accused knew the enemy would be Al-Qaeda based on the priorities of the United States and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet. This inference is reasonable considering the type of information the accused was disclosing to the website, and his training that made him aware of the type of information and the enemy's use of the Internet.

### c. C3 Document

The prosecution also offered evidence of the accused's knowledge through the Chaos Communication Congress (C3) report, which reported on the December 2009 C3 conference, an annual event that attracts hackers, security researchers, computer hobbyists and malicious computer users. The C3 report states that "the Internet is an essential communication tool for terrorists." PE 43 (C3 report). In regard to Wikileaks.org, the report explains that it is "a publicly accessible Internet Website where individuals can contact with leaked information and have it published to the public anonymously without fear of being held legally liable." *Id.* The report further states, "[t]he information that can be disclosed includes, but is not limited to, classified information, trade secrets, corporate information, personally identifiable information, and even operational data." *Id.* The report also discusses the threat from the insider leaking information to Wikileaks.org, as Mr. Julian Assange was encouraging the leaking of classified and proprietary information at the conference. Testimony of Mr. Hosburgh; *see also* PE 43 (C3 report).

The prosecution offered evidence that the accused searched for the report on 14 February 2010, just one day after returning from R&R leave. *See* Testimony of SA Shaver; PE 85 (Intelink logs). The prosecution also offered evidence that the accused moved a copy of the C3 report to his personal Macintosh computer on 15 February 2010. Testimony of Mr. Mark Johnson; PE 127 (Volumes.txt which showed the C3 document was on the accused's personal Macintosh computer).

The above evidence leads to a reasonable inference that the accused's accessing the individual report and moving it to his personal computer demonstrates that the accused read the document. Again, by reading the report, the accused was put on notice that by giving information to Wikileaks.org, a site that was quickly gaining a reputation for encouraging leaks of classified government information and a website that seemingly posted everything it received, would be used by the enemy. This is circumstantial evidence that the accused knew the enemy would be Al-Qaeda based on the priorities of the United States and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet.

### 3. Statements by accused

The prosecution introduced evidence of the accused's own statements that documented his knowledge that by giving information to Wikileaks.org, he was giving it to the enemy.

a. Chats with Mr. Adrian Lamo

The prosecution offered evidence that in his chats with Adrian Lamo, the accused called the disclosed Department of State cables "world-wide anarchy in CSV format." PE 30 (Wired.com chat logs of the accused and Mr. Lamo). The accused also asserted that the DoS cables will affect "everybody on earth." *Id.* The accused further noted that "Hilary Clinton, and several thousand diplomats around the world are going to have a heart attack when they wake up one morning, and find an entire repository of classified foreign policy is available, in searchable format to the public...=L". *Id.* It is a reasonable inference that if the accused knew that everyone in the world would have access to the information on Wikileaks.org, that the enemy, namely Al-Qaeda would have access. This information further reveals that the accused knew the value of the US government information contained in the Department of State cables, which further requires the conclusion that by disclosing that information to Wikileaks, that the accused knew he was giving the information to the enemy, as he knew the information would be valuable to the enemy.

Additionally, as pointed out in the defense brief, the accused acknowledged that he "could've sold [the information] to Russia or China, and made bank" but he did not "because it's public data" and "because another state would just take advantage of the information . . . try to get some edge." *Id.* The defense argues that this statement shows the accused's "focus was on getting certain information to the American public in order to hopefully spark change and reform." Defense RCM 917 Motion for Article 104 at 3. However, there is no evidence supports the defense interpretation of the chat, and should be left for argument. The accused never once mentions the American public or the United States being any sort of motivation for his crimes in any of his chats or emails. The statement cited by the defense instead requires the opposite conclusion, as it shows that the accused did not want to limit access to the information to one group, but wanted everyone to see the information.

b. Chats with Mr. Julian Assange

The prosecution also offered evidence that the accused (dawgnetwork) was chatting with Mr. Julian Assange (pressassociation). Testimony of Mr. Johnson; PE 120 (Buddy List from the Accused's personal computer listing pressassociation's contact information); PE 123 (Chats recovered for the accused's personal computer between pressassociation and dawgnetwork). In those chats, on 10 March 2010, the accused called Wikileaks.org the first "Intelligence Agency" for the general public. *See* PE 123 (Chats recovered for the accused's personal Mac between pressassociation and dawgnetwork). This demonstrates that the accused does not think of Wikileaks.org as a news organization. The chats with Mr. Assange also show that the accused knew the information that he transmitted to Wikileaks.org would be published on the Internet. *See* PE 123 (Chats recovered for the accused's personal computer between pressassociation and dawgnetwork). On 6 March 2010, the accused asked Mr. Assange if he was "gonna give release a shot?" Mr. Assange responded, "yes." *Id.* The accused also asks Mr. Assange, "is it like the entire world is uploading to you?" Mr. Assange responds with examples of information releases from Hungary, Haiti, and Germany, indicating the international interest in his website. *See* PE 123 (Chats recovered for the accused's personal Mac between pressassociation and dawgnetwork).



In summary, it is a reasonable inference that based on the above evidence that the accused knew the enemy used the Internet, the accused knew who the enemy was, and the accused knew the Wikileaks.org website was on the Internet and commonly contained classified official US government information and was about to contain a lot more classified government information that would be of value to the enemy courtesy of the accused.

Although not appropriate for a RCM 917 motion, the defense argues in their motion that the accused did not have actual knowledge that by giving the classified US government information to the enemy that the accused was giving the information to Wikileaks.org, the evidence supports the opposite conclusion through circumstantial evidence. Based on the evidence presented by the prosecution, it is a reasonable inference that the accused was trained by the military on the enemy (particularly Al-Qaeda and Usama Bin Laden) and its use of the Internet, the accused was trained by the military on the types of information the enemy would be seeking on the Internet, the accused was informed of how Wikileaks.org conducted business by his own searches during the commission of his misconduct, and the accused acknowledged in his discussions during the commission of his misconduct that he knew exactly what he was doing in disclosing the charged information. Ultimately, a reasonable inference can be drawn based on the circumstantial evidence that the accused knew that by giving information to Wikileaks.org, he was giving information to the enemy, specifically Al-Qaeda.

### CONCLUSION

Since the prosecution has presented evidence on every element of the Specification of Charge I (Article 104), the defense request to enter a finding of not guilty as to the Specification of Charge I should be denied. This is particularly true given the lower burden on the prosecution to withstand an RCM 917 motion and the requirement that the Court must view the evidence "in the light most favorable to the prosecution." RCM 917(c).



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on the Defense Counsel, via electronic mail, on 11 July 2013.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**GOVERNMENT RESPONSE TO  
DEFENSE MOTION FOR DIRECTED  
VERDICT: 18 U.S.C. 1030 OFFENSE**

11 July 2013

**RELIEF SOUGHT**

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the Defense Motion for Directed Verdict: 18 U.S.C. § 1030 Offense.

**STANDARD**

"A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." Rule for Courts-Martial (hereinafter "RCM") 917(d). "The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*

**WITNESSES/EVIDENCE**

The United States requests the Court consider all previous submissions by the parties relating to the offenses alleging misconduct in violation of 18 U.S.C. § 1030(a)(1) (Appellate Exhibits 90, 91, 170, and 188), the Court's two previous rulings on this issue (AEs 139 and 218), and the testimony and evidence cited herein.

**LEGAL AUTHORITY AND ARGUMENT**

"The military judge, on motion by the accused or *sua sponte*, shall enter a finding of not guilty of one or more offenses charged after the evidence on either side is closed and before findings on the general issue of guilt are announced if the evidence is insufficient to sustain a conviction of the offense affected." RCM 917(a). The motion by the accused shall state with specificity where the evidence is insufficient to enable the trial counsel to respond to the motion, and the Court shall give each party an opportunity to be heard on the matter. *See* RCM 917(b); RCM 917(c); RCM 917(c), discussion (stating that the military judge ordinarily should permit the trial counsel to reopen the case as to the insufficiency specified in the motion).

A motion for a finding of not guilty "shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." RCM 917(d). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*; *United States v. Perez*, 40 M.J. 373 (C.M.A.

1994) (upholding the military judge's decision not to enter a finding of not guilty because the testimony of three witnesses, construed in the light most favorable to the prosecution, could reasonably tend to establish the overt act). The standard of "some evidence" required to survive a motion for a finding of not guilty is a low one. See *United States v. Escochea-Sanchez*, 2013 WL 561356 (N-M. Ct. Crim. App. 2013) (concurring with the military judge who "noted repeatedly while hearing argument on the RCM 917 motion [that] the standard for surviving such a motion is very low"); *United States v. Jenkins*, 59 M.J. 893, 898 (A. Ct. Crim. App. 2004) (encouraging trial judges to view the standard used to decide whether to grant a motion for a finding of guilty as a mirror image of the standard used to decide whether to give an instruction on an affirmative defense); *United States v. Athearn*, 1994 WL 711894 (A.F. Ct. Crim. App. 1994) (noting that "[t]he military judge was obviously correct in denying the motion for a finding of not guilty under the low, 'some evidence' standard set out in R.C.M. 917(d)") (quoting RCM 917(d)). Direct or circumstantial evidence satisfies the "some evidence" standard. See *United States v. Parker*, 59 M.J. 195 (C.A.A.F. 2003); *United States v. Varkonyi*, 645 F.2d 453, 458 (5th Cir. 1981).

The defense motion for a directed verdict with respect to Specification 13 of Charge II should be denied. For the third time in this court-martial, the defense argues that the United States has failed to allege the accused "exceeded authorized access" within the meaning of 18 U.S.C. § 1030(a)(1) because the accused "was authorized to access each and every piece of information he accessed." Def. Mot. at 2; see AE 170 at 4 ("PFC Manning was authorized to access each and every piece of information he allegedly accessed"); AE 90 at 27 ("PFC Manning had access to the relevant SIPRNET computers and was authorized to access every piece of information that he allegedly accessed on the SIPRNET"). The defense argument over three separate filings is virtually verbatim—the only change is that the defense has dropped the word "allegedly." This Court has ruled that restrictions on access "can include manner of access." AE 218 at 2. In filing this motion for a directed verdict, the defense appears to have ignored the Court's statement of the law. See Def. Mot. at 3 ("That is, 'exceeds authorized access' is not concerned with the *manner* in which information to which one has access is downloaded; it is rather concerned with whether the accused was *authorized to obtain or alter the information* that was obtained or altered." ). The Government's theory for Specification 13 of Charge II is a valid application of the statute. See AE 218. The Government presented evidence in accordance with that theory during its case-in-chief, including evidence relating to each essential element. No further inquiry is necessary.

#### I. THE GOVERNMENT'S PROFFERED THEORY WAS CONSIDERED BY THE COURT.

Prior to trial, the Government proffered that the accused "exceeded authorized access" within the meaning of 18 U.S.C. § 1030(a)(1) when he obtained the information at issue using an unauthorized program (Wget). See AE 188 at 2. In that same filing, the Government stated that "Wget can be used as a 'web crawler' by extracting resources linked from web pages and downloading them in sequence...Wget can be used to rapidly mine data from websites." *Id.* The Government cited evidence presented at the Article 32 investigation, which showed that "the accused added Wget to his [SIPRNET] computer and used the program to access and harvest more than 250,000 Department of State diplomatic cables from the Net-Centric Diplomacy

(NCD) website.” *Id.* The Government proffered that evidence presented at the court-martial would establish that Wget was not authorized software for Army computers. *Id.*

Thereafter, this Court considered the proffer of the Government, *the defense legal authority and argument*, and ruled:

Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can arise from a variety of sources, to include regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive.

AE 218 at 2. This Court made it clear that criminal liability for exceeding authorized access under 18 U.S.C. § 1030(a)(1) was “not limited to code breaking restrictions on access.” *Id.*

## II. THE GOVERNMENT PRESENTED EVIDENCE IN ACCORDANCE WITH ITS PROFFERED THEORY.

The United States is puzzled. It would be one thing if the Government proffered a theory to the Court that was not borne out at trial by the facts—facts that must be viewed in the light most favorable to the prosecution. It is another thing entirely when the defense articulates, on the first page of its motion, the Court’s ruling on the issue of “exceeds authorized access” with an incomplete reference to the record and without further elaboration. *See* Def. Mot. at 1 (“The Court ruled, in response to the first motion, that the Court would adopt the narrow view of *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) such that the Government would not be able to bootstrap use restrictions (improper use of information) into access restrictions for the purposes of 18 U.S.C. § 1030.”).

As stated above, the proffered theory for “exceeds authorized access” was that the accused obtained the information at issue using an unauthorized program. For purposes of this motion, it is important to note four separate conclusions of law by this Court. First, “restrictions on access can include manner of access.” AE 218. Second, “user agreements can also contain restrictions on access as well as restrictions on use.” *Id.* Third, access and use “are not mutually exclusive.” *Id.* Finally, “exceeds authorized access” is not limited to code breaking restrictions on access.” *Id.* The defense concedes that the United States introduced evidence that the accused used the program Wget to download more than 250,000 Department of State cables. *See* Def. Mot. at 2 (“The Government has introduced evidence that PFC Manning used the program Wget to download the diplomatic cables.”). Thus, the only inquiry left is whether the prosecution presented evidence that Wget was an unauthorized program. Fortunately for the Court’s determination of this issue, the United States has presented overwhelming evidence that Wget – whether characterized as software, freeware, or an executable – was not authorized on Army computers generally, and the Defense Common Ground System-Army (DCGS-A) computers specifically. *See* Testimony of SA David Shaver (stating that Wget is not a standard

program on Army computers and was not part of the Army Gold Master, and that there is no difference between software and executables); Testimony of Mr. Jason Milliman (stating that only the DCGS-A Field Software Engineer (FSE) was authorized to put an executable file on DCGS-A machines); Testimony of CPT Thomas Cherepko (stating that the Acceptable Use Policy and AR 25-2 prohibited introducing software, freeware, or executables, and that Wget was not an authorized executable file); Testimony of Mark Kitz (stating that Wget is not on the DCGS-A baseline system, and that Wget did not go through the process and was never authorized).

### III. THE GOVERNMENT PRESENTED EVIDENCE WITH RESPECT TO EACH ESSENTIAL ELEMENT OF THE OFFENSE.

This Court must determine whether the evidence presented could reasonably tend to sustain a conviction for the relevant offense. *See* RCM 917(a). A motion for a finding of not guilty "shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." RCM 917(d). In order to find the accused guilty of Specification 13 of Charge II, the Court must find:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, the accused knowingly accessed a computer exceeding authorized access on a Secret Internet Protocol Router Network;

(2) the accused obtained information that has been determined by the United States Government by Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than 75 classified United States Department of State cables;

(3) the accused had reason to believe the information obtained could be used to the injury of the United States or to the advantage of any foreign nation;

(4) the accused communicated, delivered, transmitted, or caused to be communicated, delivered or transmitted the information to a person not entitled to receive it;

(5) the accused acted willfully; and

(6) under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

*See* AE 410.

The United States presented evidence with respect to each essential element of the offense during its case-in-chief. Although the defense did not raise the issue of whether the United States presented evidence with respect to element (3) above, the testimony of several witnesses, as well as the charged diplomatic cables themselves, establish that the accused had

"reason to believe" the cables he obtained could be used to the injury of the United States or to the advantage of any foreign nation. *See, e.g.*, Testimony of Troy Moul (AIT instruction); PEs 169-178 (diplomatic cables were marked with classification). The only other contested element is whether the accused "knowingly" exceeded authorized access on the SIPRNET. On this point, the prosecution presented overwhelming evidence that the misconduct was "knowing." SA Shaver testified that Wget was under the accused's user profile and not in the program files. Thus, the program was only available to the accused on the computer he was using. *See* Testimony of SA Shaver. SA Shaver also testified that to run Wget, the accused had to create a program or script in order to download the cables from NCD and the detainee assessments from the Intellipedia site. *Id.* Mr. Milliman, the DCGS-A FSE and administrator, was never approached to put Wget on a computer, nor had he heard of Wget before his involvement in this case. *See* Testimony of Mr. Milliman. There is also no evidence the accused asked any of his superiors whether he could download Wget to his SIPRNET computer; in fact, none of the unit witnesses testified that they even knew what Wget was until recently. *See* Testimony of Unit Witnesses. Further, the evidence showed that the accused specifically enabled private browsing in Mozilla Firefox to prevent the recording of search and activity history on the SIPRNET. *See* Testimony of SA Shaver. As such, there is overwhelming evidence that when the accused downloaded Wget and put it on his computer (on at least two separate occasions), he did so in a manner that hid the program from other users, his supervisors, and the administrator. The logical inference is that the accused knew the program was not authorized to be used to rapidly harvest more than 250,000 cables from NCD, and more than 700 detainee assessments from an Intellipedia site.

#### IV. THE EVIDENCE PRESENTED ALSO ESTABLISHED THAT WGET OR SOMETHING LIKE IT WAS NOT EMBEDDED WITHIN NET-CENTRIC DIPLOMACY.

The evidence presented established that the "manner" of accessing or obtaining the cables in this case was the use of a Wget, an unauthorized program. Wget was not part of the Department of State Net-Centric Diplomacy (NCD) website, and there was no mechanism to allow users of NCD to download or print multiple cables at one time. *See* Testimony of Charles Wisecarver; Testimony of SA Shaver (Wget was not embedded as part of the NCD server). Mr. Wisecarver also testified that diplomatic cables downloaded from NCD came with a banner embedded. *See* Testimony of Mr. Wisecarver. Although Mr. Wisecarver could not remember the exact wording of the banner, the banner reads as follows:

USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR  
UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO  
MONITORING OF THIS SYSTEM. UNLESS SPECIFICALLY  
LABELED AS RELEASABLE TO FOREIGN NATIONALS,  
CONTENT IN THIS DoS INFORMATION SYSTEM IS NOT  
RELEASABLE TO FOREIGN NATIONALS.  
UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL  
PROSECUTION. EVIDENCE OF UNAUTHORIZED USE  
COLLECTED DURING MONITORING MAY BE USED FOR

ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE  
ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT  
TO MONITORING FOR THESE PURPOSES.

*See, e.g.*, Prosecution Exhibit 173c (example of banner embedded in cables downloaded from NCD). The defense characterizes the database banner as focused on the “*use* of the information.” Def. Mot. at 10. Fortunately, the Court does not have to rely on the defense to be candid. The “*use*” in the banner above clearly refers to use of the system itself. As the Court stated, access and use “are not mutually exclusive.” AE 218. The banner can fairly be read as “unauthorized use [of this computer system] may subject you to criminal prosecution”, which is separate and apart from the prohibition on releasing “content” or information in the system to foreign nationals. It also appears the defense is attempting to confuse the Court by intimating that because Microsoft Excel was part of the baseline package for the DCGS-A machines, there was some kind of authorized mechanism the accused could have used to download cables rapidly from NCD. *See* Def. Mot. at 3. Microsoft Excel is a program used by analysts to create spreadsheets and tables. *See* Testimony of CW2 Kyle Balonek (all Soldiers within the S-2 section used Microsoft Excel spreadsheets for simple tasks). The idea that a spreadsheet program like Excel doubles as a program that could download webpages rapidly is preposterous and one example of the way the defense has mischaracterized evidence. The Court should note, however, that the Combined Information Data Network Exchange (CIDNE) database allowed a user to export significant activity reports in monthly increments to a comma separated value file or Excel file—an example of a database containing a design feature which allowed downloading in batches. *See* Testimony of Chad Madaras; Stipulation of Expected Testimony for Patrick Hoeffel (CIDNE allows a user to export SIGACTs into a “.csv” format)


V. A DECADE IN JAIL IS THE MAXIMUM PENALTY FOR A VIOLATION OF 18  
U.S.C. § 1030(a)(1).

The defense asserts at several points that a “decade in jail cannot turn on what programs the Army happens to put on its ‘authorized software’ list.” Def. Mot. at 3; *see also* Def. Mot. at 15 (“It would be a sad day indeed if a decade in jail could hinge exclusively on what program an accused used to download information he was otherwise entitled to access and otherwise entitled to download.”). Aside from whether this is an appropriate argument for a motion under RCM 917, the legislative branch determined that the maximum penalty for a violation of 18 U.S.C. § 1030(a)(1) was ten years in prison. In its focus on whether the use of “unauthorized software” should be relevant to the “exceeding authorized access” inquiry, the defense forgets that § 1030(a)(1) as a whole criminalizes serious misconduct. *See* 18 U.S.C. § 1030(a)(1) (punishing individuals who obtain and communicate classified information to unauthorized persons). Additionally, the evidence presented during the prosecution’s case-in-chief established that Wget is a dangerous program for the SIPRNET. *See, e.g.*, Testimony of CW4 Armond Rouillard (stating that he used Wget in his OPFOR capacity for attacking the Army network, and he was specifically authorized to install Wget; Wget is only for individuals who are penetration testers and OPFOR); Testimony of SA Shaver (Wget downloaded information faster than humanly possible); Testimony of CPT Cherepko (Wget “scrapes” websites and retrieves any data that is set in the program to retrieve); Testimony of Mr. Weaver (Wget allows you to do entire content

downloading of a website). Accordingly, policies prohibiting Wget on SIPRNET computers seem more than appropriate.

CONCLUSION

The United States respectfully requests this Court DENY the Defense Motion for Directed Verdict: 18 U.S.C. 1030 Offense. For the reasons stated above, the United States has presented evidence with respect to each essential element of Specification 13 of Charge II.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 11 July 2013.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )

PFC, U.S. Army, )

HHC, U.S. Army Garrison, )

Joint Base Myer-Henderson Hall )

Fort Myer, Virginia 22211 )

Prosecution Notice

Potential Rebuttal Case

15 July 2013

### RELIEF SOUGHT

The prosecution in the above case respectfully requests the Court permit the United States to elicit the below-listed information to rebut the evidence raised in the defense case in chief. See RCM 913(c).

### STANDARD

"It is well settled that the function of rebuttal evidence is to explain, repel, counteract or disprove the evidence introduced by the opposing party." *United States v. Banks*, 36 M.J. 150, 166 (C.M.A. 1992) (quoting *United States v. Shaw*, 26 C.M.R. 47, 51 (C.M.A. 1958) (Ferguson, J., dissenting)). "The scope of rebuttal is defined by evidence introduced by the other party." *Id.* (citations omitted).

### FACTS

The prosecution rested on 2 July 2013. The defense rested on 10 July 2013.

### WITNESSES/EVIDENCE

SPC Kyra Marshall  
Mr. Allen (Jason) Milliman  
SA David Shaver  
Ms. Jihreah Showman  
Additional Forensic Investigator/Witness

### POTENTIAL REBUTTAL

The United States will re-call Ms. Showman to rebut the motive evidence the defense elicited from Ms. Lauren McNamara (formerly known as Mr. Zachary Antolak) in the February 2009 to August 2009 (pre-deployment) timeframe.

The United States will call SPC Marshall to rebut the motive evidence the defense elicited from SGT Sadtler in the March 2010 (deployment) timeframe.



The United States will re-call SA Shaver to discuss a specific SIGACT, dated March 2010 to expound upon and counteract the testimony of SGT Sadtler that he thought the incident that the accused approached him with documentation about, involving Iraqi Nationals being arrested, may have taken place in December 2009.

The United States will re-call SA Shaver to discuss emails the accused sent to members of the media, as well as Wikileaks tweets that were found on the accused's personal Macintosh computer, to rebut the evidence offered by the defense that Wikileaks operated as a journalistic organization, and was considered a legitimate journalistic organization elicited through Professor Yochai Benkler.

The United States will re-call SA Shaver to discuss how Wget was run from the accused's profile on his SIPRNET computer to counteract the testimony of CW2 Ehresman that executable files could be run off of a disk.

The United States will re-call an additional forensic investigator/witness to discuss how the Wikileaks.org website appeared in 2009 and 2010 to expound upon and counteract the evidence offered by the defense that Wikileaks operated as a journalistic organization elicited through Professor Yochai Benkler.

The United States will re-call Mr. Milliman to explain what was and was not authorized on the DCGS-A machines. Specifically, he will testify that he would not have told CW2 Ehresman that he could run otherwise unauthorized programs and executable files from a CD.

The United States will request the Court take judicial notice of the entire book, *Good Soldiers*, by David Finkel to explain what the accused would have read in the book beyond the select portions of which the Court took judicial notice and admitted upon defense request.

Depending on the defense disclosures pursuant to RCM 914, the United States may re-call additional defense witnesses or others in rebuttal.

#### CONCLUSION

Since the above-listed evidence goes directly to explain or contradict evidence raised by the defense in their case in chief, the prosecution should be permitted to raise the evidence in rebuttal.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on the Defense Counsel,  
via electronic mail, on 15 July 2013.

  
ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx-xxxx )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO**

**GOVERNMENT RESPONSE**

**TO MOTION FOR DIRECTED**

**VERDICT ON THE 18 U.S.C. §641  
OFFENSES**

DATED: 12 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty for Specifications 4, 6, 8, and 12 of Charge II.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

**A. The Government's Apparent Contention that "Database = Records = Copies of Records = Information" Must be Rejected**

3. After reading the Government's Response, the Defense still has no idea what the Government is saying it has charged PFC Manning with "stealing" or "converting" within the meaning of 18 U.S.C. §641. To the best of the Defense's ability to understand the Government's position, it appears to be saying it has charged PFC Manning with stealing the databases *and* the records contained in the database (and/or their copies) *and* the information contained in the records.<sup>1</sup> See

<sup>1</sup> The Defense cannot figure out what this means for the Government's position on valuation. It appears that since the Government is arguing that databases contain records which contain information, it is allowed to aggregate the value of the database *with* a value of the records *with* a value of the information contained in the records. See Government Motion, p. 20 ("Similarly, evidence of the cost of production for the databases and records contained therein cannot be separated from the information because the information requires protection.") If this is the Government's position, there is *no case* dealing with §641 that has permitted a theory of this nature to proceed. Cases have allowed the prosecution to proceed separately with *either* charging/proving theft of "records" (or copies of records, as the case may be) or theft of "information." No court has ever allowed a prosecution to proceed based

Government Motion (“the accused stole and converted the databases and records listed in the § 641 specifications” (p. 2); “the evidence proves the contents of the databases and the records were stolen or converted” (p. 2); “The United States charged that the accused compromised databases, to include the records contained in the databases” (p. 12); “the records include the information contained therein” (p. 13); “The accused both stole and converted the information he compromised” (p. 14); “The accused’s admission provides a reasonable inference of his intent to deprive the United States Government permanently of the records and information contained therein” (p. 15); “the conveyance harmed the United State’s [sic.] interest in exclusive possession of the information in the records, thereby further adding to the conversion caused by the accused.” (p. 16); “The accused stole and converted records maintained on United States Government computer systems” (p. 17); “any distinction between copies of the records is feckless” (p. 17); “the accused is charged with stealing or converting databases, to include the records contained therein, and not documents” (p. 19)).

4. In short, it seems like the Government wants the word “database” to encapsulate everything under the sun—records, copies of records, information in records, and the exclusive possession of information contained in records. The problem for the Government is that it simply charged PFC Manning with stealing “databases” —not records, not copies, not information, or any variation thereof. Neither records, nor copies of records, nor information, is fairly embraced within the word “database.” The Government’s last-ditch and schizophrenic attempt to argue that the word “database” encapsulates all these other things (things which have independent meaning and value) must be rejected.

5. The Government’s position seems to be that the relevant databases (CIDNE, NCD, SOUTHCOM) are coextensive, or synonymous, with the records that are housed in the database and, by further extension, the information that is contained within those records within the database. See Government Motion, p.13 (“By the plain meanings of the § 641 specifications, the records include the information contained therein. A database is ‘a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means.’ Black’s Law Dictionary (9th ed. 2009). Similarly, a record is ‘information that is inscribed on a tangible medium or that, having been stored in an electronic or other medium, is retrievable in perceivable form.’ Black’s Law Dictionary (9th ed. 2009). The Charge Sheet informed the accused of the stolen *res* because the Charge Sheet described stolen records, which, by definition, includes the information in those records.”). The fact that “database” is a different word than “record” indicates that the two are different things. The fact that “information” is also a different word than “database” and “record” further denotes that information is a different thing than a record or a database.

6. A database is a receptacle or container for information. If not populated with any records or information at all, it still remains a database—albeit an empty database. In this case, the databases contained things other than government records. They contained electronic means of searching, various fields, program commands and the like. If, for instance, there were no SIGACTs populating the CIDNE database, it would still be the CIDNE database. Similarly, if there were no cables populating the NCD database, it would still be the NCD database. Thus, a

---

on an amalgam of records and information. And, lest it be forgotten, the Government has not charged either “records” or “information.”

database is far *more than* the records that it may contain at a given point in time. This is such a common sense proposition that the Government's own motion, while purporting to elide "database" and "records," in fact sharply distinguishes between them. *See* Government Motion ("The Court took judicial notice that WikiLeaks posted records *from* the CIDNE-Iraq database, CIDNE-Afghanistan database, and USSOUTHCOM database. SA Bettencourt confirmed that WikiLeaks posted the purported Department of State records *from* the NCD database." (p. 3); "This SD card contained a picture of the accused, in addition to more than 380,000 records *from* the CIDNE-Iraq database" (p. 3); The SD card with which the accused stored the records *from* the CIDNE-Iraq database (p. 4); SA Shaver testified that the accused stole, purloined, or knowingly converted more than 90,000 records *from* the CIDNE-Afghanistan database" (p. 7); "...used Wget to retrieve more than 700 records *from* the United States Southern Command database accessible through the Joint Task Force–Guantanamo (JTF-GTMO) Detainee Assessment Branch website on Intellipedia. ... Mr. Jeffrey Motes confirmed that the records in the United States Southern Command database were stored by "DocumentID" and that the above database consisted of over 700 records" (p. 8); "The United States charged that the accused compromised databases, to include the records *contained in* the databases" (p. 12)). The fact that the Government repeatedly acknowledges that records are "from" certain databases, or that records are "contained in" certain databases establishes that the two (database and records) are not the same thing. Records are "contained in" databases; records "come from" databases. Records themselves, even when aggregated, are not databases.<sup>2</sup>

7. Moreover, the Government's argument that "databases = records" falls flat when one specifically considers the charged CIDNE databases. The Government alleges, for instance, that PFC Manning stole the CIDNE-Iraq and CIDNE-Afghanistan databases because he compromised thousands of records in the databases. What the Government fails to mention is that CIDNE-Iraq and CIDNE-Afghanistan databases had much more content than simply the SIGACTS. They contained, according to various witnesses, other records such as Human Intelligence Reports, Counter Improvised Explosive Device Reports, Psychological Operations Reports, etc. Thus, perhaps only 10% (for sake of argument) of the records contained within the database were copied and compromised. This fact alone demonstrates that there is a clear distinction between "database" and "records" – and that compromising certain records within the databases does not amount to stealing or converting the database itself.

## **B. The Government Must Now Own What it Pled in the Charge Sheet**

8. As indicated in the Defense's Motion for a Directed Verdict, and the Government does not dispute, the Government has charged that PFC Manning stole *databases*. The Government has never charged that PFC Manning stole copies of records<sup>3</sup> or that he stole information. When the Defense asked for elaboration on what PFC Manning is alleged to have stolen in the Defense's

<sup>2</sup> Since the Government fails to understand the difference between a database and the contents of a database, perhaps another example will be of assistance. Westlaw is a legal database containing, among other things, cases, legislation, and commentary. If a person copied every single case, statute, journal article, etc. from Westlaw onto CD, they have not have stolen the database. They may have stolen, perhaps, a copy of the various items in the database (i.e. a copy of the contents of the database). But they have not stolen the database itself—the template, the search queries, the programming code, or the items contained in the database.

<sup>3</sup> The Government bizarrely does not believe there is a distinction between records and copies of records when it is clear from all §641 case law that there is a marked difference between the two.

Motion for a Bill of Particulars, the Government maintained that “is clear what property is at issue,” namely “specific, identified databases.” In full, the Government’s position was as follows:

The defense request for particulars in paragraph 10a of the defense motion attempts to restrict the Government’s proof at trial. The defense relies on *Newman* for the proposition that a bill of particulars may be used to “clarify the specific theory upon which the Government intends to rely.” (Def. Mot. at 5.) That language or proposition does not appear in the opinion, nor is the United States aware of any authority that suggests such a wide-reaching purpose for a bill of particulars. The defense also asserts that the specifications at issue under this paragraph make the accused susceptible to unfair surprise at trial. *In fact, the specification is clear—the accused is on notice that the United States alleges he stole, purloined, or knowingly converted Government property.* As a practical matter, “steal” and “purloin” have the same meaning under the law. *United States Attorneys’ Manual, Criminal Resource Manual at 1639*, [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm01639.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01639.htm). Any argument the accused will be misled or paralyzed by decisions over what evidence to present to refute whether conduct constituted “stealing” or “knowing conversion” is without merit. *Furthermore, the theft-related offenses alleged in this case are of specific, identified databases. There is no danger the accused will be subject to prosecution for the same offense at a later date because each specification is clear regarding what property is at issue.*

Appellate Exhibit XIV (emphasis added). Thus, when the Defense sought to clarify the property that was allegedly stolen, it was told in no uncertain terms: “the theft-related offenses alleged in this case are of specific, identified databases.” *Id.*

9. The Court held that:

... the purposes of a bill for particulars are to:

- a. inform the accused of the nature of the charge(s) with sufficient precision to enable him to prepare for trial;
- b. avoid or minimize the danger or surprise at the time of trial; and
- c. enable the accused to plead acquittal or conviction in bar of another prosecution when the specification itself is too vague and indefinite for such purpose.

Appellate Exhibit XXIX. The Court then concluded that “[t]he Government responses to the Defense Request for Bill of Particulars are sufficient to satisfy the purpose of a Bill of Particulars.” *Id.* It is clear from the Bill of Particulars that the Government was alleging that PFC Manning stole “specific, identified *databases*” – not copies of records, or information. This was the charge that the court said held “sufficient precision” to enable PFC Manning to prepare for trial.

10. The Government, in fact, has always maintained that it is the *databases* that were stolen—not the records or the information contained within the records. This is clear when one looks at the Government’s proposed Instructions<sup>4</sup>:

**Specification 4 of Charge II: Violation of the UCMJ, Article 134**

In Specification 4 of Charge II, the accused is charged with stealing or converting the Combined Information Data Network Exchange Iraq *database* containing more than 380,000 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, the accused did knowingly and willfully steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: the Combined Information Data Network Exchange Iraq *database* containing more than 380,000 records;

(2) That the CIDNE-I *database* belonged to the United States government or a department or agency thereof;

(3) That the CIDNE-I *database* was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchmark*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

Lesser-Included Offense

The offense of stealing or converting the CIDNE-I *database*, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 4 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the CIDNE-I *database*, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or

<sup>4</sup> This is the Government’s proposed instruction for the CIDNE database. The additional specifications are identical except that they name other databases (CIDNE-Afghanistan Database; Net-Centric Diplomacy Database; United States Southern Command Database).

converting the CIDNE-I *database*, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the value element. The offense charged, and the lesser-included offense of stealing or converting the CIDNE-I *database*, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the CIDNE-I *database* is worth more than \$1,000.

Adapted from *Benchmark*, paragraph 2-5-10.

See Appellate Exhibit 199 (emphasis added). In this instruction, the Government referred to the charged “database” a total of *nine* times. It is crystal clear from the Government’s proposed instructions that it sought to allege the theft or conversion of the databases. It is equally clear that the Government sought to value the databases. See *id.* (“That the CIDNE-I database was of a value of more than \$1,000;”). This is fundamentally different than saying that copies of “records” had a value of more than \$1,000 or that “information” had a value of more than \$1,000.

11. Now, at the 11<sup>th</sup> hour, after the close of evidence by both parties, the Government seeks to concoct a charge which requires a string of assumptions: when we charged *databases*, we really meant the records *in the databases*, and when we meant the records in the databases, we really meant the *copies of records in the database*, and when we meant the copies of records in the database, we really meant *information in the copies of the records in the databases*, and when we meant the information in the copies of the records in the databases, we really meant the *United State’s [sic] interest in exclusive possession of the information in the records*. See Government Motion at p. 16. None of this is even remotely encapsulated in the Charge Sheet, the Bill of Particulars, or in the Government’s Instructions. It is a gargantuan leap to go from “databases” to “the United State’s [sic] interest in exclusive possession of the information in the records.”<sup>5</sup>

12. The Court, during extensive motions argument, heard the repeated refrain from the Government that “words matter” and that the Defense must provide “specificity.” The Court will recall the incident where the defense requested “documents” from Quantico, but the Government did not believe that “emails” were encapsulated within the word “documents” and thus did not produce the emails pursuant to the Defense’s discovery request. The Court will also recall the Defense asking for “investigative reports” or “damage assessments” during discovery. The Government responded that it did not have any investigative reports and that what the Defense was looking for was “working papers.” The Court will also recall the Government’s distinction between a “draft” and an “interim” report with respect to the Department of State

---

<sup>5</sup> The Government seems to think that the Defense should have objected to the Government’s introduction of certain evidence regarding valuation of information and that the failure to do so means that the Defense believed the evidence was relevant. The Government is mistaken. In the *Marshall* case, it is doubtful that the defense counsel stood up and said, “Hey Government, why are you putting forward all this evidence on CPT Kreitman when it’s clear that my client escaped from SSG Fleming? You should put forward evidence on SSG Fleming.” *United States v. Marshall*, No. 08-0779 (C.A.A.F. 2009). So too is the case here. It would be ineffective assistance of counsel for the Defense to point out that the Government’s evidence was irrelevant. It is not the job of the Defense to point out any inadequacies in the Government’s proof.



damage assessment. In each of these instances, the Government vehemently maintained that “words matter.” Well, words matter the most when we are dealing with charging documents. The 18 U.S.C. §641 offenses carry with them a total of 50 years in prison. If “emails” are not “documents” and a “draft” is not an “interim report”, then neither is a “database” a “record” or “information.” The Government has pled that PFC Manning stole databases and that is what it must prove (and what the Defense maintains it has not done).

13. The Government took almost one full year to draft the charges in this case. It could have, and should have, conducted research into the 18 U.S.C. §641 offenses. If it had, it would have realized that “records” and “information” are not the same thing in terms of the property allegedly taken (as discussed in more detail below); and they certainly are not the same thing in terms of valuation. The Government undoubtedly charged “database” because it was clear to the Government that databases generally cost millions of dollars to set up and run. Thus, the Government believed it would easily clear the \$1000 valuation hurdle. However, it failed to consider what is apparently obvious to everyone else except the Government: PFC Manning did not steal or convert the *database* itself. The Government itself now appears to concede that PFC Manning did not steal the database, but rather certain records contained therein. *See* Government Motion, p. 12 (“The United States *charged that the accused compromised databases*, to include the records contained in the databases. *See* Charge Sheet. The United States admitted evidence to provide a reasonable inference *the records* were stolen and converted.”); the Government did not argue that it proved that the databases themselves were stolen).

14. Since the Government charged PFC Manning with stealing or converting databases, it must now own what it pled and prove that PFC Manning stole or converted databases (not copies of records or information). The Court has previously held that the Government must prove what it pled and this instance is no different. *See* Appellate Exhibit 515 (“The Government elected to charge the communication under the ‘information clause.’ That clause carries with it the ‘reason to believe’ scienter requirement. The Government is required to prove beyond a reasonable doubt that the accused had reason to believe the communicated information could be used to the injury of the U.S. or to the advantage of any foreign nation...”).

**C. The Government Fails to Address 18 U.S.C. §641 Case Law Because Case Law Makes Clear that “Records” and “Information” Are Different Things**

15. What is glaringly absent from the Government’s motion is *any attempt* to grapple with, or distinguish, any of the case law cited by the Defense dealing specifically with 18 U.S.C. §641. Instead, the Government focuses extensively on a case dealing the wire and mail fraud. *See* Government motion at p. 15, 16, and 19. The reason for this is obvious: the §641 case law goes decidedly against the Government and its position in this case.

16. The Government’s legal position on its premise that “records” includes “information” is replicated, in its entirety, below:

*3. Information as part of records comports with precedent*

Charging records and the information contained therein comports with applicable precedent in criminal law. The contents and information contained in government

records determines the criminality of the theft of the records more than the form of the records. See *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), cert. denied, 385 U.S. 974 (1966) (“When the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owners should be deemed immaterial.”); *United States v. Lambert*, 446 F.Supp. 890, 894 (D.C. Conn. 1978). Under § 641, the transmission of the information contained in documents is just as larcenous as theft of the documents themselves. *United States v. Rosner*, 352 F.Supp. 915, 922 (D.C.N.Y. 1972) (noting that the importance of information in documents described in *Bottone* applies to § 641 charges).

Government Motion at p. 13-14. The Defense does not dispute that “[c]harging records and the information contained therein comports with applicable precedent in criminal law.” *Id.* The problem is that the Government did *not* charge “the information contained therein.” The Government simply charged the theft of the databases. Similarly, the Defense also does not take issue that “[u]nder § 641, the transmission of the information contained in documents [can be] just as larcenous as theft of the documents themselves.”<sup>6</sup> The Government is not saying anything remarkable here. However, if the Government has not charged *the information*, it cannot then seek to convict PFC Manning on the basis that he stole or converted the information.<sup>7</sup>

17. The Government has not addressed any of the Defense’s cases which point out that when the government is relying on the theft of “information,” the word “information” appears in the Charge Sheet or Indictment. See e.g. *United States v. Jeter*, 775 F.2d 670, \*680-1 (6<sup>th</sup> Cir. 1985) (“The government charged that Jeter ‘did willfully and knowingly embezzle, steal, purloin and convert to his own use and the use of others, and without authority did sell, convey and dispose of records and things of value of the United States, the value of which is in excess of \$100.00, to wit, carbon paper and *the information contained therein* relating to matters occurring on October 5, 1983, before a grand jury’”).

18. The Government has pointed to *no case* where a court has held that “information” is somehow fairly embraced in the word “record” for the purposes of 18 U.S.C. § 641. In fact, the cases are all to the contrary. In those courts that have accepted that information, as an intangible, is within the ambit of 18 U.S.C. § 641, they have done so on the basis that information is a “thing of value”—not that information is a “record.”<sup>8</sup> See 18 U.S.C. § 641 (“Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or *thing of value* of the United States ...”);

<sup>6</sup> To clarify, the Defense contests that § 641 applies to the theft of information (an intangible); however, the Defense acknowledges that there is legal authority in the form of case law to suggest that information can be charged as being in the ambit of the section.

<sup>7</sup> The Government is simply mistaken when it says, “The contents and information contained in government records determines the criminality of the theft of the records more than the form of the records.” See Government Motion at p. 13-14. The theft of “information” is no more criminal than the theft of “records” under 18 U.S.C. § 641. They are simply alternate charges under § 641. See e.g. *United States v. Jeter*, 775 F.2d 670, (6<sup>th</sup> Cir. 1985) (accused was charged with stealing carbon paper of a grand jury indictment, along with the information itself).

<sup>8</sup> Those courts that do not accept that information falls within the ambit of § 641 do not believe that information is “a thing of value”, much less “a record” within the statute’s terms.

See *United States v. DiGilio*, 538 F.2d 972, 978, fn 10 (3<sup>rd</sup> 1976) (“The government obviously did not consider this merely a theft of information case, because the indictment charges defendants only with converting to their use government records. Section 641 also prohibits conversion of any ‘thing of value’, and the government would presumably rely on this term in an information case”); *United States v. Jordan*, 582 F.3d 1239, 1246 (11<sup>th</sup> Cir. 2009) (indictment under §641 alleged that defendant’s “delivered the printouts which as property of the United States had a value in excess of \$1000”; in a separate count, indictment alleged that defendant received “a thing of value of the United States, that is, information contained in the NCIC records.”); *United States v. Girard*, 601 F.2d 69, 71 (D. Conn. 1979) (“we are impressed by Congress’ repeated use of the phrase “thing of value” in section 641 and its predecessors. ... The word “thing” notwithstanding, the phrase is generally construed to cover intangibles as well as tangibles. ... Although the content of a writing is an intangible, it is nonetheless a thing of value”).

19. The fact that cases have uniformly held that information falls under the “thing of value” prong of 18 U.S.C. §641 belies any interpretation that information is fairly encapsulated within any of the other words in the section—“record, voucher, money.” *Id.* In other words, the fact that courts rely on “thing of value” to describe information means that information is not encapsulated within the word “record” under 18 U.S.C. §641. Thus, even if the Government had charged PFC Manning with stealing or converting “records” (which it did not—it charged databases), it has not charged him with stealing or converting “information.” See also *United States v. Fowler*, 932 F.2d 306, 309-310 (4<sup>th</sup> Cir. 1991) (“Fowler was not charged with conveying abstract information. He was charged with conveying and converting documents, which, although copies, were things of value and tangible property of the United States. True, the documents contain information, but this fact does not deprive them of their qualities as tangible property and things of value.”).

#### **D. The Government Tries to Hide the Fact that “Records” and “Copies” Are Fundamentally Different for the Purposes of 18 U.S.C. §641**

20. The Government seeks to gloss over the fact that “records” and “copies of records” are two very different things in terms of identifying the actual property that was allegedly stolen or converted and valuing that property. See *United States v. Morison*, 844 F.2d 1057, 1077 (4<sup>th</sup> 1988) (distinguishing between theft of original information versus theft of copies: “Those cases involved copying. The defendant’s possession in both cases was not disturbed. This case does not involve copying; this case involves the actual theft and deprivation of the government of its own tangible property.”); See also *United States v. Hubbard*, 474 F. Supp. 64, 79 (D.C.D.C. 1979) (indictment charging the defendant with stealing “documents and photocopies thereof”; “therefore the indictment’s claim that the defendants violated section 641 by copying government documents through the use of government equipment withstands the defendants’ motion to dismiss because government-owned copies were taken...”).

21. The Government’s position on this reads, in its entirety:

The accused stole and converted records maintained on United States Government computer systems. The Defense argues that a fatal variance exists because the

Charge Sheet specifies records and not copies of records. See Defense 641 Motion ¶ 4. The records compromised by the accused are the records maintained by the United States. The United States maintained copies of the records because they were digitally stored on United States Government computer systems. In this case, any distinction between copies of the records is feckless because the records were stored digitally. See *DiGilio*, 538 F.2d at 978 (referring to theft of copies as “an asportation of records owned by the United States”) (emphasis added). This distinction cannot be a material variance because it does not change the nature of the offense, let alone substantially change the nature of the offense, increase the seriousness of the offense, or the punishment of the offense. Thus, any variance is not material.

Moreover, any variance between a digital record and a digital copy of the same record is not prejudicial. The distinction does not place the accused at risk of another prosecution because the accused is charged with stealing and converting the actual records, which he in fact stole and converted. Nor did the distinction affect the accused’s ability to prepare his defense because the United States charged the accused with stealing and converting the records using a term, “database,” the accused himself used to describe the records he compromised.

Government Motion at p. 17. The Defense is not really sure what the Government is saying. Is the Government saying that PFC Manning stole the actual original records? Or is the Government saying that PFC Manning stole digital copies (i.e. that he downloaded the records onto CDs and then released those digital copies) but that the distinction is not relevant for the purposes of §641? Since there is no evidence that PFC Manning took the original digital records, the Defense will assume that the Government concedes that PFC Manning took a copy but believes there is no appreciable difference between an original and a copy. See *id.* (“In this case, any distinction between copies of the records is feckless because the records were stored digitally”).

22. Whether one steals an original or a copy is of crucial significance to an 18 U.S.C. §641 prosecution. This is readily apparent when one considers the valuation prong of the section. The Government has failed to even attempt to address any of the Defense’s cases drawing a sharp distinction between valuing a *copy* of a document, and valuing the *original*. See e.g. *United States v. DiGilio*, 538 F.2d 972, 977 (3<sup>rd</sup> Cir. 1976)(court held that the “a duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen.” In terms of valuing this duplicate copy, the court held: “Irene Klimansky availed herself of several government resources in copying DiGilio’s files, namely, government time, government equipment and government supplies.”);<sup>9</sup> *United States v. Hubbard*, 474 F. Supp. 64 (D.C.D.C. 1979) (court allowed prosecution to proceed on theory that “the copies, allegedly made from government documents, by means of government resources, are records of the

<sup>9</sup> The Government cites *DiGilio* apparently for the proposition that it “refer[s] to theft of copies as “an asportation of records owned by the United States.” *Id.* (emphasis in original). The Defense is not sure how this helps the Government at all. In *DiGilio*, the court distinguished between original records and copies of records. It held that the copies of records made by the accused with government resources were themselves “records” within the meaning of the statute and that these copies needed to be valued. This is exactly the position of the Defense.

government , and thus the copies were stolen). Thus, whether PFC Manning stole “records” or “copies of records” is not something that the Government can simply sweep under the rug as essentially “no big deal.” What PFC Manning allegedly stole or converted, and its value, will determine whether he will face five separate convictions carrying with them fifty years of potential imprisonment.


23. As stated in the Defense’s original motion, if the allegedly stolen or converted property is a copy of a record, then it is the value of the copy that must be established (e.g. the cost of the CD, the time spent copying, the use of government servers for the copying, etc.). The Government has introduced no evidence of the value of the copies allegedly stolen or converted in this case. It cannot rely on the value of the originals to establish the value of the copies.

### CONCLUSION

24. The Government claims that there is no difference between a “database,” a “record,” a “copy of a record”, or “information.” Unfortunately, a database does not equal a record does not equal a copy of a record does not equal information. All of these are different things. And the Government must own what it charged: the databases. It is too late in the game, after the close of evidence, to explain what it “really meant.” The Government had the Charge Sheet to explain what it “really meant.” It had the Bill of Particulars to explain what it “really meant.” It had the Instructions to explain what it “really meant.” What it really meant is that PFC Manning stole certain databases. Full stop. If, in its mind, it conflated databases with copies of records with information, that is not the Defense’s problem. The Defense was on notice that it had to defend against a charge that PFC Manning stole or converted certain “databases.” PFC Manning did no such thing. Accordingly, the Defense renews its request for a finding of not guilty.<sup>10</sup>

25. The role of the Court is not to help the Government to clean up the mess it has created. The role of the Court is to determine, by looking at applicable federal case law, whether the Government has introduced any evidence of what it has charged: that PFC Manning has stolen or converted certain databases. And the Defense submits that it has not.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

---

<sup>10</sup> If the Court does not grant this R.C.M. 917 motion and allows the Government to proceed with some variation of “records” or “information,” the Defense will likely file an additional R.C.M. 917 motion seeking to dismiss the offense for lack of proof and/or to challenge whether “information” is properly within the ambit of §641.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

) AMENDMENT #2  
) DRAFT  
) INSTRUCTIONS:

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

) DATED: 15 July 2013

For the specification of Charge I, (Aiding the Enemy, in violation of Article 104, UCMJ), the Government advised the Court that it is not offering evidence that PFC Manning knowingly gave intelligence to a classified entity specified in Bates Number 00410660-00410664. Accordingly, the Court makes the following amendment to element (1) in the Instruction for the specification of Charge I at AE 410:

Change:

Current Instruction: "(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, the accused, without proper authority, knowingly gave intelligence information to certain persons, namely: al Qaeda, al Qaeda in the Arabian Peninsula, and an entity specified in Bates Number 00410660 through 00410664 (classified entity);"

Amended Instruction: "(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, the accused, without proper authority, knowingly gave intelligence information to certain persons, namely: al Qaeda and al Qaeda in the Arabian Peninsula;"

So ORDERED this 15<sup>th</sup> day of July 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

**David Coombs**

---

**From:** Joshua E <oc4romeos@yahoo.com>  
**Sent:** Friday, June 21, 2013 12:32 AM  
**To:** David Coombs  
**Subject:** Re: Question

Sir,  
I do not remember who said it, i do know that it was put out to me when i got there in November. So it was prior to me arriving.

**From:** David Coombs <[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)>  
**To:** 'An Irish Lad' <[oc4romeos@yahoo.com](mailto:oc4romeos@yahoo.com)>  
**Sent:** Thursday, June 20, 2013 8:16 PM  
**Subject:** Question

Chief,

I wanted to ask you a follow up question on what you told me during our last conversation. You had told me that the S2 Section permitted soldiers to place a shortcut for an executable file on the desktop of the DCGS-A computers or to run an executable file from a CD on their DCGS-A computers. Do you recall when this guidance was put out? Also do you recall who might have said that this was permitted? Thank you.

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government Brief  
on 18 U.S.C. § 641  
and Intangible Property,  
to include Information

17 July 2013

#### RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion for Directed Verdict: Charge II, Specifications 4, 6, 8, 12 and Defense Motion for Directed Verdict: Specification 16 of Charge II because the United States has presented evidence for each element of each specification.

#### BURDEN OF PERSUASION AND BURDEN OF PROOF

"A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." Rule for Courts-Martial (hereinafter "RCM") 917(d). "The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*

#### FACTS

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice (hereinafter "UCMJ"). The accused is also charged with causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, UCMJ, eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641 (hereinafter "§ 641"), two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications alleging misconduct in violation of Article 92 of the UCMJ. *See* Charge Sheet.

The accused pleaded guilty by substitutions and exceptions to Specifications 2, 3, 5, 7, 9, 10, 13, 14 and 15 of Charge II. *See* Appellate Exhibit (hereinafter "AE") CDXLIV. The accused did not plead guilty, *inter alia*, to Specifications 4, 6, 8, 12, and 16 of Charge II (hereinafter "§ 641 specification"). *See id.*

#### WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States requests that the Court consider the Charge Sheet, Prosecution Exhibits (hereinafter "PE"), testimony, and the Appellate Exhibits (hereinafter "AE") cited herein.

606



## LEGAL AUTHORITY AND ARGUMENT

The Defense argues that information does not fall within the ambit of § 641. The Defense argument fails because United States Circuit Courts of Appeal have broadly applied “thing of value” to information. § 641 reaches theft and conversion beyond the limitations of common law. Thus, the precedent regarding § 641 holds that information is a “thing of value.”

### I. DATABASES AND RECORDS ARE UNITED STATES GOVERNMENT PROPERTY

#### A. Accused Compromised Databases and the Records Therein

The accused is charged with the theft or conversion of databases consisting of a number of records. *See* Charge Sheet. The evidence creates a reasonable inference that the accused used United States Government systems to create the records he conveyed to WikiLeaks. *See, e.g.*, Testimony of David Shaver; Testimony of SA Williamson; PE 30; PE 50; PE 82; PE 83; PE 92; PE 104. Where an accused avails himself of United States Government equipment to create copies, those copies remain records and property of the United States. *United States v. Hubbard*, 474 F. Supp 64, 79 (D.C. Cir. 1979); *United States v. DiGilio*, 538 F.3d 972, 978 (3d Cir. 1976). The Third Circuit decided:

[The accused] availed herself of several government resources in copying DiGilio's files, namely, government time, government equipment and government supplies. That she was not specifically authorized to make these copies does not alter their character as records of the government. A duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen.

*Id.* Because the accused utilized United States Government systems to compromise the charged databases, to include their records, the database and records the accused compromised remained records of the United States. The United States did not retain these records; thus, Defense arguments that the United States retained possession of the records is moot because the Defense mistakes which records were actually stolen and converted. *Cf. United States v. Matzkin*, 14 F.3d 1014, 1020-21 (4th Cir. 1994) (holding that the United States need not have the sole interest in a bid for it to be information that is a “thing of value” under § 641). Furthermore, electronic property that can later be reduced to a tangible form is protected under § 641. *See United States v. Morris*, 284 Fed. Appx. 762, 762-63 (11th Cir. 2008) (upholding a conviction under § 641 for theft of money where funds were directly deposited into an account).

#### B. Information Is an Intrinsic Quality of the Databases and Records

Information comprises an intrinsic quality of the compromised databases and records. The information contained in databases and records can be used to authenticate them as evidence. *See* Military Rule of Evidence 901(b)(4). The information dictates the market price for the information. *See* Testimony of Mr. Lewis. The statutory reference to “any record” includes the information held in the record and database. *United States v. Lambert*, 446 F. Supp.

890, 896 (D.C. Conn. 1978), *aff'd*, *United States v. Girard*, 601 F.2d 69, 70 (2d Cir. 1979). In *Lambert*, the Court found:

The phrase “other thing of value” strongly suggests that something other than the particular records themselves, i.e., the contents, are probably covered as well. Indeed, the distinction between a government “record” and its contents is rather fine. The individual of common intelligence would probably include the information held in a government computer in the statutory term “record” without reference to the catch-all phrase “thing of value.”

*Id.* Therefore, the court held that an accused planning the unauthorized asportation of information held in a government data bank possessed sufficient notice that § 641 covered such conduct. *Id.* Also, the accused signed a non-disclosure agreements (hereinafter “NDAs”) that gave the accused notice that classified information is the property of the United States Government. See PE 59 ¶ 7; PE 60 ¶ 7. The NDAs gave the accused additional notice that § 641 applies to unauthorized disclosure of classified information. See PE 59 ¶¶ 4, 10; PE 60 ¶¶ 4, 10. Here, where the contents of the databases and records could be used to authenticate the charged property, the information affected the value of the charged property, the individual of common intelligence in 1979, before computers were as widely used, would conclude that a record includes information, and the accused signed NDAs stating that classified information is the property of the United States Government, the accused had sufficient notice of the charged property.

## II. A “THING OF VALUE” UNDER § 641 INCLUDES INFORMATION

§ 641 makes criminal the theft or conversion of a “thing of value.”<sup>1</sup> § 641. “A ‘thing of value’ can be tangible or intangible property.” AE CDX. Government information, although intangible, “is a species of property and a thing of value.” *Id.*

### A. The Supreme Court Established the Broad Reach of § 641

In discussing the pertinent legislative and judicial history of § 641 and similar crimes, the Supreme Court observed that “the modern tendency is to broaden the offense of larceny, by whatever name it may be called, to include such related offenses as would tend to complicate prosecutions under strict pleading and practice. *United States v. Morissette*, 342 U.S. 240, 270 & n.28 (1952). The Court added that stealing and purloining were added “to cover such cases as may shade into larceny, as well as any new situation which may arise under changing modern conditions and not envisioned under common law . . . .” *Id.* Thus, § 641 applies to “acts which shade into crimes but which, most strictly considered, might not be found to fit their fixed definitions.” *Id.* In particular, § 641 closed the “gaps” and “crevices” that allowed guilty men to escape criminal liability. See *id.* at 271. (“What has concerned codifiers of the larceny-type

<sup>1</sup> In pertinent part, § 641 states, “Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States . . . [s]hall be fined under this title or imprisoned not more than ten years, or both . . . .” 18 U.S.C. § 641.

offense is that gaps or crevices have separated particular crimes of this general class and guilty men have escaped through the breaches. The books contain a surfeit of cases drawing fine distinctions between slightly different circumstances under which one may obtain wrongful advantages from another's property."). To close the gaps, Congress included the word "steal," a word "having no common law definition to restrict its meaning as an offense, and commonly used to denote any dishonest transaction whereby one person obtains that which rightfully belongs to another, and deprives the owner of the rights and benefits of ownership . . ." See *id.* (emphasis added).

Military courts also recognize the expansive scope of a thing of value. See, e.g., *United States v. Ward*, 35 C.M.R. 834, 837 (A.F.B.R. 1965) (stating that a "thing of value" under Article 123a, UCMJ, extends to every kind of right or interest in property, or derived from contract, including interest and rights which are intangible or contingent or which mature in the future). Since 1962 military courts distinguish between an "article of value," which is based on the strict common law concept of larceny, and a "thing of value," which encompassed a broader scope upon its implementation. See generally *United States v. Mervine*, 26 M.J. 482, 483-84 & nn.1-2 (C.M.A. 1988) (explaining that statutes may enlarge the scope of larceny, but the drafters declined to do so for Article 121, UCMJ). Here, the Supreme Court has found that Congress drafted § 641 to fill the gaps and capture all types of larcenies. See *Morissette*, *supra*. Thus, a "thing of value" should be given its all-encompassing meaning with respect to the § 641 specifications. See Part II.B.C.1, *infra*.

Additionally, "[t]he military is a notice pleading jurisdiction." *United States v. Fosler*, 70 M.J. 225, 229 (C.M.A. 2011) (citing *United States v. Sell*, 3 C.M.A. 202, 206 (C.M.A. 1953). "A specification is a plain, concise, and definite statement of the essential facts constituting the offense charged. A specification is sufficient if it alleges every element of the charged offense expressly or by necessary implication." RCM 307(c)(3). "An accused must be given notice as to which clause or clauses he must defense against . . ." RCM 307(c)(3), discussion (citing *United States v. Fosler*, 70 M.J. at 229. In *Morissette*, the Supreme Court held that § 641 possessed a broad reach under "strict pleading and practice." *Morissette*, 342 U.S. at 270 n.28. Therefore, the broad reach of § 641 recognized in *Morissette* is more appropriate for the notice practice used in military practice.

#### B. "Thing of Value" Includes Information

A "thing of value" includes intangible and tangible property. AE CDX; see, e.g., *United States v. Jeter*, 775 F.2d 670 (6th Cir. 1985); *Girard*, 601 F.2d at 70. Accordingly, four Circuit Courts of Appeal explicitly agree that a "thing of value" under § 641 includes information. The Second Circuit held that the information reduced to writing in a document constituted an intangible "thing of value" under § 641. *Girard*, 601 F.2d at 70-71. The Sixth Circuit concluded information comprises government property or a "thing of value" under § 641. *Jeter*, 775 F.2d at 680-82. Noting its agreement with the Second and Sixth Circuits, the Fourth Circuit similarly determined that information is a "thing of value" under § 641. *United States v. Fowler*, 932 F.2d 306, 310 (4th Cir. 1991) (holding that conversion and conveyance of governmental information can violate § 641). The Eleventh Circuit upheld a conviction under § 641 for conveying information in United States Government records. *United States v. Jordan*, 582 F.3d 1239, 1246

(11th Cir. 2009). Similarly, the Third Circuit has found meritorious the argument that interference with the exclusive use of information established a sufficient basis for criminal liability under § 641. *DiGilio*, 538 F.3d at 978 (finding merit to the Government's argument that a misappropriation of information falls under § 641 but declining to so hold where a technical larceny was already proven).

Furthermore, additional circuits have held that § 641 embraces intangible property. The Seventh Circuit has found the testimony of a witness to be a "thing of value." *United States v. Zouras*, 497 F.2d 1115, 1121 (7th Cir. 1974) (finding a "thing of value" under 18 U.S.C. § 876 to include testimony); see also *United States v. Croft*, 750 F.2d 1354, 1359-62 (7th Cir. 1984) (holding that § 641 applies to conversion of a student's services for a personal research project). The District of Columbia Circuit held that a "thing of value" under § 641 applied to conversion of computer time and storage. *United States v. Collins*, 56 F.3d 1416, 1418-19 (D.C. Cir. 1995). The Eighth Circuit decided that a "thing of value" reached a right in the intangible property of flight time. *United States v. May*, 625 F.2d 186, 191-92 (agreeing with *DiGilio* and *Girard*, *supra*). In sum, in addition to the four Circuit Courts of Appeal that hold information to be an intangible "thing of value" under § 641, three additional Circuit Courts of Appeal apply a "thing of value" broadly to intangible property. Therefore, a "thing of value" under § 641 applies to information.

#### C. Precedent Cited by the Defense Inapposite

##### 1. § 641 Reaches Beyond Common Law Definitions

A single Circuit Court of Appeals has held that a "thing of value" should be applied only to tangible items. See *Chappell v. United States*, 270 F.2d 274, 277 (9th Cir. 1959). However, in 1986 the same Court that decided *Chappell*, citing criticism of the "limited, narrow, and unrealistic interpretation" of a "thing of value" under § 641 "reject[ed]" its prior decision *sua sponte*. *United States v. Schwartz*, 785 F.2d 673, 680-81 & n.4 (9th Cir. 1986) (citing *United States v. Croft*, 750 F.2d 1354, 1362 (7th Cir. 1984)). In "rejecting" *Chappell*, the Ninth Circuit stated that it had "tended clearly toward a broader scope of a *thing of value*, to include intangibles." *Id.* (italics in original) (citing *United States v. Sheker*, 618 F.2d 607, 609 (9th Cir. 1980)) (holding information to be a "thing of value" under 18 U.S.C. § 912); *Friedman*, 445 F.2d at 1084-85; *Whaley v. United States*, 324 F.2d 356 (9th Cir. 1963) (holding implicitly information to be a "thing of value"). Moreover, the Ninth Circuit noted that legislative history cited in *Schwartz* undermined the decision in *Chappell*. *Id.* Therefore, the Ninth Circuit joined other Circuit Courts of Appeals in finding a "thing of value" to be unambiguous, and therefore not requiring the rule of lenity. See *Schwartz*, 785 F.2d at 681 (finding error in applying rule of lenity to a "thing of value" under § 1954).

After deciding *Schwartz*, the Ninth Circuit supported its *Chappell* holding in *United States v. Tobias*, 836 F.2d 449 (9th Cir. 1988). The Ninth Circuit distinguished the legislative history of 18 U.S.C. § 1954 in *Schwartz* as part of the basis for its renewed support for *Chappell*. *Tobias*, 836 F.2d at 451 n.2. *Schwartz* and *Tobias* were decided by different Circuit judges, and any split exists only within the Ninth Circuit. Additionally, in *Tobias*, the Ninth Circuit acknowledged the existence of the "intangible goods" exception or "classified information"

exception to § 641” but did not invoke the so-called “exceptions” because they were inapplicable to the tangible property at issue in *Tobias*. See *id.* at 451.<sup>2</sup>

The Ninth Circuit’s holdings in *Chappell* and *Tobias* and Judge Winter’s dissent in *United States v. Truong Dinh Hung*, 629 F.2d 908, 924-28 & n.21 (Winter, J., dissenting as to application of § 641), contradict the Supreme Court’s holding in *Morissette*. Judge Winter, however, acknowledged that § 641 could be applied to theft of United States Government information on “a case-by-case basis.” *Truong Dinh Hung*, 629 F.2d at 928 (citing *Lambert*, 446 F. Supp. at 899).<sup>3</sup> In *Chappell*, the Ninth Circuit relied on the common law definition of “conversion” to restrict application of § 641 only to tangible goods. *Chappell*, 270 F.2d at 277 (“As Congress must have known, the words ‘converts’ and ‘conversion’ really have their origin in the law of torts. The terms imply a dealing with goods or personal chattels.”). Citing a discussion of trover and conversion, the Ninth Circuit narrowed the scope of § 641. See *id.* at 277-78 (citing *Olschewski v. Hudson*, 87 Cal. App. 282 (Cal. App. 1927)).

In *Morissette*, the Supreme Court decided that § 641 covered common law larceny and “any new situation which may arise under changing modern conditions and not envisioned under the common law. . . .” *Morissette*, 342 U.S. at 270 n.30 (emphasis added). Specifically, the Supreme Court held that Congress broadened the reach of § 641 by adding “purloin” and “steal,” the latter which has “no common law definition to restrict its meaning as an offense.” *Id.* (emphasis added). At common law, trover would lie for the unlawful taking or conversion of a chattel or personal property. See, e.g., *Granfinanciera, S.A. v. Nordberg*, 492 U.S. 33, 44 (1989) (citations omitted); *United States v. Loughrey*, 172 U.S. 206, 212 (1898); *Johnson v. Weedman*, 4 Scam. 495 (Ill. 1843). Reverting to common law construction, the Ninth Circuit frustrates Congressional intent and binding precedent by ignoring the modern terms used by Congress. These terms, “steal” and “purloin,” lack any common law restrictions. *Morissette*, 342 U.S. at 270 n.30. Accordingly, the Supreme Court held that “[t]he history of § 641 demonstrates that it was to apply to acts which constituted larceny or embezzlement at common law and also acts which shade into those crimes but which, most strictly considered, might not be found to fit their fixed definitions.” *Id.* (emphasis added). The Ninth Circuit, applying the common law definition of “conversion” appends such a “fixed definition.” Therefore, imputing the common law application of “conversion” defeats the purpose of § 641. See *id.*

## 2. Other Defense Precedent Inapplicable Here

Cited by the defense, *Pearson v. Dodd*, 410 F.2d 701, 703 (D.C. Cir. 1969) involved a claim for the tort of invasion of privacy. Publishing a matter in the general public interest is a defense to the tort of invasion of privacy by the publication. *Id.* *Pearson* is inapplicable because it pertained to the persons who received copies of documents without authorization, not the person who conveyed the documents without authorization. *Id.* at 705. Because *Pearson*

<sup>2</sup> In *Tobias*, the items at issue were cryptographic cards who value came from their use as devices. *Tobias*, 836 F.2d at 452. Both parties agreed that the devices did not contain information, and the Ninth Circuit accordingly treated the device solely as tangible property. See *id.* at 451-52.

<sup>3</sup> Judge Winter does not explain the factors that would make application of § 641 to information appropriate in his opinion. See *Truong Dinh Hung*, 629 F.2d at 928.

analyzes tort law with respect to persons receiving documents, it is not germane to this court-martial. See *id.* at 705 (“[W]here the claim is that private information concerning plaintiff has been published, the question of whether that information is genuinely private or is of public interest should not turn on the manner in which it has been obtained.”).<sup>4</sup>

Additional material cited by the Defense similarly offers no persuasive value. Professor Nimmer’s article and comment notes that no copyright exists in United States Government documents. Melville B. Nimmer, *National Security Secrets v. Free Speech, The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311, 320 (1974) (analyzing 17 U.S.C. § 8). Having stated that no copyright exists in United States Government documents, Professor Nimmer argues that the criminal penalties set forth in 17 U.S.C. § 8—the penalties for copyright infringement—should apply to United States documents. See *id.* at 320-21 (acknowledging that Congress can criminalize copying certain United States Government documents). This incongruous argument offers no persuasive value. Indeed, as Professor Nimmer recognizes, Congress can protect information in documents and has enacted legislation to criminalize certain copying. See *id.* (noting that 18 U.S.C. § 793(b) “has made some copying criminal”).

Finally, the Defense presents *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) for the proposition that § 641 does not capture the theft or conversion of information. In *Morison*, the Fourth Circuit determined that *United States v. Carpenter*, 484 U.S. 19 (1987), resolved the issue and held that “pure ‘information’” may be the subject of statutory protection under § 641. See *Morison*, 844 F.2d at 1077. The Fourth Circuit added that illegally disposing of United States Government records and photographs to a third party constituted “a textbook application of the crime set forth in § 641.” *Id.* The Defense highlights *Morison*’s reference to *Pearson*, but the reference is inapposite as set forth above and in Part I because, in the instant matter, the databases and records the accused asported were not returned. See *Morison*, *supra*; *Hubbard*, *supra*.

### III. RULE OF LENITY

Military courts apply the rule of lenity when construing ambiguous criminal statutes. AE CXXXIX (citing *United States v. Schelin*, 15 M.J. 218, 220 (C.M.A. 1983); *United States v. Cartwright*, 13 M.J. 174, 176 & n.4 (C.M.A. 1982); *United States v. Inthavong*, M.J. 628, 630 (A. Ct. Crim. App. 1998)). The rule of lenity “requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.” AE CXXXIX (citing *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006)). The rule of lenity, however, does not preclude a theory of prosecution that employs “well-known” understandings of the statutory terms. See *Romm*, 455 F.3d at 1001 (holding that the government’s theory fell within the plain meaning of the language of the criminal statute). Accordingly, the rule of lenity may be applied “only if, after reviewing all sources from which legislative intent may be gleaned, the statute remains truly ambiguous.” *Inthavong*, 48 M.J. at 630 (citing *United States v. Davis*, 656 F.2d 153, 158 (5th Cir. 1981)).

#### A. Statutory Language Supports Inclusion of Information as a “Thing of Value”

<sup>4</sup> In *Pearson*, the appellee was a United States Senator, and the court held that the published information “clearly bore on the appellee’s qualifications as a United States Senator.” *Pearson*, 410 F.2d at 703.

The starting point for statutory interpretation is the plain or ordinary meaning of the language. See *United States v. McCollum*, 58 M.J. 323, 340 (C.A.A.F. 2003); *United States v. James*, 63 M.J. 217, 221 (C.A.A.F. 2006) (stating that “a fundamental rule of statutory interpretation is that ‘courts must presume that a legislature says in a statute what it means and means in a statute what it says there’”) (citing *Connecticut Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992)). When a statute is clear and unambiguous, courts need not and should not consult the legislative history. *Ratzlaf v. United States*, 510 U.S. 135, 147-48 (1994) (“[W]e do not resort to legislative history to cloud a statutory text that is clear.”).

The statutory definition of a “thing of value” is clear and unambiguous. A “thing” is “the subject matter of a right, whether it is a material object or not; any subject matter of ownership within the sphere of proprietary or valuable rights.” Black’s Law Dictionary (9th ed. 2009). Proprietary information comprises a property and right of ownership. See *Carpenter*, 484 U.S. at 25 (recognizing as worthy of protection a property right in confidential business information). Thus, information is a property right under the plain meaning of a “thing of value.” The Supreme Court supported this finding when it determined that “stealing” captures any transaction depriving an owner of rights and benefits. See *Morissette*, 72 U.S. at 270 n.28. To the extent the Ninth Circuit rejects this plain meaning, it does so by reference to “conversion,” which is a separate and distinct term. Moreover, the Supreme Court rejected limiting § 641 to common law definitions. See *id.* Therefore, the Ninth Circuit’s holding in *Chappell* contradicts *Morissette* but does not contradict the plain meaning of a “thing of value.”<sup>5</sup>

Although the statutory text and legislative history support the interpretation of the United States in this case, the simple existence of some statutory ambiguity is not sufficient to warrant application of the rule of lenity. *Muscarello v. United States*, 524 U.S. 125, 138 (1998). Most statutes are ambiguous to some degree; consequently, the “mere possibility of articulating a narrower construction...does not by itself make the rule of lenity applicable.” *Id.* (quoting *Smith v. United States*, 508 U.S. 223, 239 (1993)). The Supreme Court has stated that “the rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a ‘grievous ambiguity or uncertainty in the statute,’ such that the Court must simply guess as to what Congress intended.” *Barber v. Thomas*, 130 S. Ct. 2499, 2508-09 (2010) (quoting *Muscarello*, 524 U.S. at 139). In this case, there is no grievous ambiguity or uncertainty.

## B. Legislative and Judicial History Supports the United States’ Theory

Assuming, *arguendo*, the statutory text is ambiguous, the relevant legislative history and precedent confirm the United States’ interpretation of § 641 and a “thing of value.”<sup>6</sup> As described above in Part II.B-C, six Circuit Courts of Appeal have applied a “thing of value” to intangible property. Moreover, four Circuit Courts of Appeal have applied a “thing of value”

<sup>5</sup> The Ninth Circuit reinterprets “conversion,” whose definition need not be decided to determine what constitutes a “thing of value.”

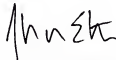
<sup>6</sup> The United States makes this argument based on *Morissette*’s interpretation of the legislative history. The United States has been unable to locate the legislative history. To obtain the legislative history, the United States would have to send an attorney to the Library of Congress. The United States offers to obtain the legislative history if it would please the Court.



specifically to "information," and a fifth Circuit Court of Appeal found merit to the United States' argument presented herein. Furthermore, as described in Part II.C.1, the Ninth Circuit's ruling in *Chappell* contradicts legislative intent of the scope of § 641 as detailed in *Morissette*. See generally *Lambert*, 446 F. Supp. At 893-95 (describing a more flexible approach for interpreting § 641 as appropriate given *Morissette*). In particular, *Chappell* creates the types of "gaps" and "crevices" Congress sought to preclude by enacting § 641. See *Morissette*, *supra*. Therefore, applying "thing of value" to reach "information" follows legislative intent and judicial precedent and rather released to unauthorized individuals.

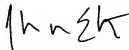
#### CONCLUSION

The Defense argues that information does not fall within the ambit of § 641. The Defense argument fails because United States Circuit Courts of Appeal have broadly applied "thing of value" to information. § 641 reaches theft and conversion beyond the limitations of common law. Thus, the precedent regarding § 641 holds that information is a "thing of value."



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 17 July 2013.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel



LOOK INSIDE!

Kindle Book

Print Book

Zoom — Zoom +



The Good Soldiers  
(Hardcover)

by David Finkel

★ ★ ★ ★ ★ (159)

Hardcover \$10.40

Add to Cart

Want it **Wednesday, July 17?** Order within 17 hrs 13 mins and choose One-Day Shipping.

35 used & new from \$1.50

Book sections

Front Matter

Cover Page

Table of Contents

First Pages

Surprise Me

Search Inside This Book



## A NOTE ON SOURCES AND METHODS

Most of this book is based on events I personally observed between January 2007, when I first met the 2-16, and June 2008, the month of the Ranger Ball. I spent a total of eight months with the 2-16 in Iraq and made additional reporting trips to Fort Riley, in Kansas; Brooke Army Medical Center, in San Antonio, Texas; the National Naval Medical Center, in Bethesda, Maryland; and Walter Reed Army Medical Center, in Washington, D.C.

The book also contains some scenes for which I wasn't present. In those instances, the details, descriptions, and dialogue used in the book were verified through internal army reports, photographs, videos, after-the-fact observation, and interviews with as many participants as conditions would permit. All of the people described and quoted in the book knew that I was a journalist and that everything I was seeing and hearing was on the record.

It is to the army's credit, I believe, that during the length of my reporting, there were only two times that I was asked to treat something as off the record. Both requests involved classified technological applications in use by the soldiers, the revealing of which could conceivably put subsequent soldiers using the applications at increased risk, and I agreed to do so.

And it is to the 2-16 soldiers' credit that they tolerated a journalist being among them, and in almost all cases welcomed me with their trust. From the beginning, I explained to them that my intent was to document their corner of the war, without agenda. This book, then, is that corner, unadorned. I feel privileged to have been its witness, and to write the story of what happened.

**Fein, Ashden MAJ USARMY MDW (US)**

---

**From:** David Coombs [coombs@armycourtartialdefense.com]  
**Sent:** Wednesday, July 17, 2013 5:34 PM  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** Tooman, Joshua J CPT USARMY (US); Hurley, Thomas F MAJ USARMY (US); Bennett, Jessica D SSG USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Mitroka, Katherine F CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); USARMY Ft McNair mdw Mailbox MDW Court Reporters OMB; Raffel, Michael J SFC USARMY (US); Parra, Jairo A (JP) CW2 USARMY USAMDW (US); Fein, Ashden MAJ USARMY MDW (US)  
**Subject:** Additional Case for Defense Filing  
**Attachments:** U.S. v. Veloria.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Completed

Ma'am,

I have attached an ACCA case that I will reference during tomorrow 641 argument.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**RULING: Defense Motions  
For Findings of Not Guilty -  
RCM 917**

**18 July 2013**

---

On 4 July 2013, the Defense filed four Motions for Findings of Not Guilty in accordance with (IAW) RCM 917 for the following offenses alleging that the Government has failed to present evidence to prove one or more elements of those offenses (AEs 593-596).

(1) Aiding the Enemy, in violation of Article 104, UCMJ (the specification of Charge 1). The Defense challenges one element and specifically asserts the Government has not provided evidence that proves the accused knowingly gave intelligence information to certain persons, namely: al Qaeda, and al Qaeda in the Arabian Peninsula. The Court's instructions define "knowingly." "'Knowingly' requires actual knowledge by the accused that by giving the intelligence to the 3<sup>rd</sup> party or intermediary or in some other indirect way, that he was actually giving intelligence to the enemy through this indirect means. This offense requires that the accused had a general evil intent in that the accused had to know he was dealing, directly or indirectly, with an enemy of the United States. 'Knowingly' means to act voluntarily and deliberately. A person cannot violate Article 104 by committing an act inadvertently, accidentally, or negligently that has the effect of aiding the enemy."

(2) Fraud and Related Activity with Computers, in violation of 18 U.S.C. §1030(a)(1) and Article 134, UCMJ (specification 13 of Charge 11). The Defense asserts the Government has not provided evidence that the accused exceeded authorized access on a Secret Internet Protocol Router Network (SIPR) computer;

(3) Stealing, Purloining, or Knowingly Converting Records Belonging to the United States, in violation of 18 U.S.C. §641 and Article 134, UCMJ (specifications 4, 6, 8, 12, and 16 of Charge 11);

(4) Particularized motion with respect to specification 16 of Charge 11.

On 11 July 2013, the Government filed three briefs in opposition (AEs 599-601). On 12 July 2013, the Defense filed a reply brief to the Government's brief in response to the Defense Motion for a Finding of Not Guilty on the 18 U.S.C. §641 offenses (AE 603). On 16 July 2013, the Defense supplemented their brief on the 18 U.S.C. §641 offenses with an email filing (AE 608). On 17 July 2013, the Government filed a supplemental response in opposition to the email filing (AE 606). On 15 July 2013, the Court heard oral argument on the RCM 917 Motions for the specification of Charge 1 (Aiding the Enemy, in violation of Article 104, UCMJ) and specification 13 of Charge 11 (Fraud and Related Activities with Computers, in violation of

18 U.S.C. §1030(a)(1) and Article 134, UCMJ). On 18 July 2013, the parties will present oral argument regarding the RCM 917 Motions for specifications 4, 6, 8, 12, and 16 of Charge II (Stealing, Purloining, or Knowingly Converting Records Belonging to the United States, in violation of 18 U.S.C. §641 and Article 134, UCMJ).

This ruling sets forth the legal standard used by the Court in determining motions for a finding of not guilty under RCM 917 and findings of fact and conclusions of law regarding the RCM 917 motions for Article 104, Aiding the Enemy and 18 U.S.C. §1030(a)(1)/Article 134. After hearing oral argument on the motions, the Court will issue a supplemental ruling for the 18 U.S.C. §641/Article 134 offenses.

#### **The Law:**

1. PFC Manning has elected trial by military judge alone, thus, the Court acts in two capacities. As the fact finder, the court must determine whether the Government has proven each and every element of each offense charged beyond a reasonable doubt. In considering this Motion for a finding of Not Guilty by the Defense, the Court acts in its interlocutory capacity and decides the motion under the lesser standard required in RCM 917.
2. RCM 917 Standard: A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged. The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses. RCM 917(d).
3. Should the Court grant a finding of not guilty to an element of the greater offense for an offense to which PFC Manning has pled guilty to a lesser included offense, the Government would be precluded from proceeding on the greater offense. RCM 917(e).

#### **RCM 917 – Article 104, UCMJ, Aiding the Enemy:**

##### **Findings of Fact:**

1. The Court has examined the prosecution exhibits, defense exhibit J, and testimony of the witnesses set forth in the Witnesses/Evidence portion of the Government brief (AE 600). This provides some evidence that between on or about 1 November 2009 and 27 May 2010 the accused:

(1) was an enlisted Soldier who was a trained all-source intelligence analyst (35F). The accused trained and passed 35F Advanced Individual Training (AIT). This training identified al Qaeda as a terrorist group. It also included a lesson on terrorist use of the internet and lessons on information security (INFOSEC) to include the classification process, why information is classified, restrictions on access to classified information, storage and safekeeping of classified information to include individual responsibility to safeguard classified information and to ensure that unauthorized persons do not gain access to classified information. The training further instructed 35F Soldiers that the enemy will attempt to discover how and when the U.S. is

conducting operations. As such, critical information (anything that helps the enemy obtain an advantage over the U.S.) including tactics, techniques and procedures (TTPs), unit capabilities and intent, and personal/family information must be protected. The training completed by the accused warned that operational activities should not be discussed on the internet or on email, and Soldiers should always assume the adversary is reading posted material.

(2) prepared a slide show dated 13 Jun 08 entitled "Operations Security (OPSEC)" that defined critical information, identified adversaries, listed common OPSEC leaks, and concluded with the need to avoid public disclosure of critical information to include posting information on the internet.

(3) signed two non-disclosure agreements dated 7 April 2008 and 17 September 2008, respectively, where he acknowledged that he received and understood a security indoctrination concerning the nature and protection of classified information including the procedures to be followed in ascertaining whether persons to whom the accused contemplates disclosing classified information have been approved for access to it and that the accused has been advised that the unauthorized disclosure of classified information could cause damage or irreparable injury to the U.S. or could be used to the advantage of a foreign nation.

(4) maintained a variety of intelligence publications on his external hard drive. Portions of the publications address use of the internet by terrorist organizations and opposing forces.

(5) deployed to Forward Operating Base (FOB) Hammer, Iraq on or about October 2009 and remained deployed there past May 2010. He had access to the classified information on the Secret Internet Protocol Router (SIPR) network on the Defense Common Ground System-Army (DCGS-A) computers in the 2<sup>nd</sup> Brigade (BDE) SCIF. The accused was working as an all-source intelligence analyst, using the sigacts on the CIDNE-I database to develop intelligence products that involved pattern analysis. The accused downloaded, indexed, and plotted CIDNE-I sigacts on maps based on locations and enemy threats. The accused was aware that the enemy also engaged in similar pattern analysis about U.S. TTPs and movements. The accused sent to WikiLeaks the same CIDNE-I database and sigacts he used to develop pattern analysis with the intent that it be disclosed to the public.

(6) accessed the ACIC report published on 18 March 2008 entitled "Wikileaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" on 1 December 2009, 29 December 2009, 1 March 2010 and 7 March 2010. The ACIC report was a counterintelligence analysis report analyzing the threat posed by Wikileaks.org following the release of 2000 pages of U.S. Army Tables of Equipment in Iraq and Afghanistan from April 2007 and release of other classified U.S. information. The report listed as an intelligence gap "Will the Wikileaks.org Web site be used by FISS, foreign military services, foreign insurgents, or terrorist groups to collect sensitive or classified U.S. Army information posted to the Wikileaks.org Web site?". The report also listed a conclusion that "It must be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the Wikileaks.org Web site. Web sites similar to Wikileaks.org will continue to proliferate and will continue to represent a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army for the foreseeable future." The accused sent the ACIC report

to Wikileaks between on or about 15 February 2010 and 15 March 2010 with the intent that it be disclosed to the public.

(7) on 14 February 2010 searched for IRR 5 391 0014 08 dated 23 March 2008 entitled "Internet Web Postings of Classified and for Official Use Only Documents". The IRR discussed Wikileaks as a publicly accessible Internet website where leaked information, including classified information, can be published to the public anonymously. The report described the threat to the Marine Corps of publication of Marine Corps sensitive or classified information. On 15 February 2010, the accused moved the IRR to his personal computer.

(8) on 14 February 2010, searched for a report dated 7 January 2010 entitled "MARFOREUR TRIP REPORT (MTR) discussing Marine Corps monitoring of Chaos Communication Congress 26C3 Here Be Dragons Conference held 26-30 December 2009." The report discussed the conference discussion on Wikileaks as a publicly accessible Internet website where leaked information, including classified information, can be published to the public anonymously. On 15 February 2010, the accused moved the MTR to his personal computer.

(9) made statements in his 5 – 18 March 2010 chats with Press Association/Julian Assange indicating his understanding that WikiLeaks was "like an intelligence agency minus the anonymous sources" and that WikiLeaks was seeking to publish Government controlled information sent to them by the accused and other donors.

(10) made statements in his May 2010 chats with Adrian Lamo admitting that he gave WikiLeaks the following classified information from the SIPRNET: a database of half a million events during the Iraq war...from 2004-2009...with reports, date time groups, lat-lon locations, casualty figures, 260,000 state department cables from embassies and consulates all over the world, classified cable from U.S. embassy Reykyavik on Icesave dated 13 Jan 10, the Gharani airstrike video from CENTCOM.smil.mil; the Apache video, and the JTF-GTMO papers. The accused also made statements that the 260,000 classified cables from the Net-Centric Diplomacy database that he sent to WikiLeaks would be released to the public in searchable format.

#### **Conclusion of Law:**

The accused's training and experience as an all source intelligence analyst, his preparation of intelligence products while deployed in Iraq, a combat zone, using the CIDNE-I database while contemporaneously sending the entire database to WikiLeaks for public disclosure and worldwide publication, the volume of classified information from the Department of Defense and the Department of State that the accused admitted to disclosing to WikiLeaks, and the accused's search for and downloading of counterintelligence documents reporting the threat posed by WikiLeaks, considered together, provide some evidence from which, together with all reasonable inferences and applicable assumptions, viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses, could reasonably tend to establish that the accused actually knew he was dealing with the enemy and actually knew that by sending such information to WikiLeaks with the intent that it be broadcast to the public, he was knowingly providing intelligence to the enemy. The "intelligence gap" evidence in the ACIC report as well

as laudable motive evidence by the accused goes to the weight of the evidence, a decision properly determined by the fact-finder.

## **RCM 917 – 18 U.S.C. §1030(a)(1), Fraud and Related Activity with Computers**

### **Findings of Fact:**

1. The Government's theory for specification 13 of Charge II is that the accused "exceeded authorized access" by accessing and downloading classified information using Wget, unauthorized software on Army computers and on the DCGS-A computers.
2. 18 U.S.C. §1030(e)(6) defines the phrase "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." There is a split in the federal circuits regarding whether this definition is an access only restriction or whether a restriction on use of the information accessed can violate the statute as well. *See generally Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston*, 87-JAN Fla. B.J. 36 (January 2013).
3. This Court has issued two previous rulings dated 8 June 2012 (AE 139) and 18 July 2012 (AE 218) in response to Defense Motions to Dismiss specifications 13 and 14 of Charge II. In those rulings, the Court found ambiguity in the statute, applied the rule of lenity, and ruled that the Court would instruct in accordance with the narrow interpretation that "exceeds authorized access" is limited to violations of restrictions on access to information and not restrictions on the use of information. The Court specifically ruled "Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can come from a variety of sources, to include regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive. The Court does not find this issue capable of resolution prior to the presentation of evidence. These issues are properly decided after the formal presentation of the evidence as a motion for a finding of not guilty or a motion for finding that the evidence is not legally sufficient."
4. The accused pled guilty to lesser included offenses of specifications 13 and 14 of Charge II. The Government advised the Court it is not going forward with the greater offense for specification 14 of Charge II.
5. In line with the Court's 18 July 2012 order, the Defense challenges the Government theory on legal grounds and moves for a Finding of Not Guilty. Specifically, the Defense argues that there were no restrictions on the accused's access to the Department of State (DOS) Net-Centric Diplomacy (NCD) database or his ability to download the records in the NCD imposed by either DOS or DoD. The accused would have the same access to the NCD whether he used Wget to download the files rapidly or whether he downloaded them slowly by click/save. Thus, the Defense argues, even if Wget is an unauthorized program, it is not an access restriction for purposes of 18 U.S.C. §1030(a)(1).

6. The Defense cites *Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963 (D.N.H.), a civil case under 18 U.S.C. 1030(a)(2)(C) where the defendants violated a hospital computer use policy by connecting large removable storage devices to download information. The court held that this was a use restriction not an access restriction ("Of course, the distinction between an employer-imposed "use restriction" and an "access restriction" may sometimes be difficult to discern, since both emanate from policy decisions made by the employer – decisions about who should have what degree of access to the employer's computer and stored data and, once given such access, the varying uses to which each employee may legitimately put those computers and the data stored on them. But, simply denominating limitations as "access restrictions" does not convert what is otherwise a use policy to an access restriction. Here, the hospital's policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access. An employee who is given access to hospital data need not "hack" the hospital's computers or circumvent technological access barriers in order to impermissibly copy that data onto an external storage device. The offending conduct in this case is misuse of data the employee was authorized to access, not an unauthorized access of protected computers and data.")

7. The Government has presented testimony by Special Agent (SA) David Shaver, Mr. Jason Milliman, CPT Thomas Cherepko, and Mr. Mark Kirtz that Wget is not authorized software for a DCGS-A computer and, even if it was, Wget, as executable software, was required to be installed by Mr. Milliman on the DCGS-A computers. The Government has also presented evidence that the accused downloaded Wget to his user profile on the DCGS-A computer he used in the SCIF.

8. The Defense has elicited testimony from Mr. Weaver and COL Miller that Wget was no different than executable software such as games, and, even if technically prohibited, these prohibitions were not enforced by the chain of command.

#### **Conclusions of Law:**

1. The Court adheres to its rulings on interpreting "exceeding authorized access" in AE 139 and 218.
2. Unlike *Wentworth-Douglass Hospital*, this case involves classified information belonging to the U.S. government. The accused is charged under 18 U.S.C. §1030(a)(1). Although the definition for "exceeds authorized access" is the same for all of the sections of 18 U.S.C. 1030, access restrictions on classified information can be more stringent than for other information and can include manner of access restrictions designed to ensure the security and protection of the classified information and to prevent the classified information from exposure to viruses, trojan horses or other malware.
3. Evidence that the accused used unauthorized software, Wget, to access and download the classified records charged in specification 13 of Charge II provides some evidence from which,



together with all reasonable inferences and applicable assumptions, viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses, could reasonably tend to establish that the accused "exceeded authorized access" on a SIPR computer. The countervailing evidence presented by the Defense goes to the weight of the evidence, a decision properly determined by the fact-finder.

**Ruling:** The Defense Motions for a Finding of Not Guilty for the specification of Charge 1 and specification 13 of Charge II are **Denied**. The Court will issue a supplemental ruling regarding the Defense Motions for a Finding of Not Guilty for Specifications 4, 6, 8, 12, and 16 of Charge II in due course.

So **Ordered** this 18th day of July 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

**Property****Value of Property**

Database	—————→	Cost of Production – Equip & Maint
Records	—————→	Cost of Production Original
Copies of Records	—————→	Cost of Production Copy
Information	—————→	Thieves' Market

**Property****Value of Property**

Database	—————→	Cost of Production – Equip & Maint
Records	—————→	Cost of Production Original
Copies of Records	—————→	Cost of Production Copy
Information	—————→	Thieves' Market

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REQUEST FOR  
SPECIAL FINDINGS UNDER  
ARTICLE 51(d) OF THE  
UNIFORM CODE OF MILITARY  
JUSTICE AND R.C.M. 918(b)**

DATED: 19 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 918(b) and Article 51(d) of the Uniform Code of Military Justice (UCMJ), requests this Court to enter special findings for the following specifications: The Specification of Charge I, Specification 1 of Charge II, Specification 4 of Charge II, Specification 6 of Charge II, Specification 8 of Charge II, Specification 11 of Charge II, Specification 12 of Charge II, Specification 16 of Charge II, and Specifications 1-4 of Charge III. The Defense also requests the Court to enter special findings for the following greater offenses: Specification 2 of Charge II, Specification 3 of Charge II, Specification 5 of Charge II, Specification 7 of Charge II, Specification 9 of Charge II, Specification 10 of Charge II, Specification 13 of Charge II, and Specification 15 of Charge II.

STANDARD

2. Pursuant to Article 51(d) of the UCMJ and R.C.M. 918(b), in a trial by a court-martial composed of a military judge alone, the military judge is required to make special findings of fact under request.

ARGUMENT

3. The defense requests that the Court enter special findings for the specifications and charges listed above when it announces its general findings. The Court, as a general rule, should make special findings on all matters upon which members would be instructed. *United States v. Falin*, 43 C.M.R. 702 (A.C.M.R. 1971); *see also United States v. Truss*, 70 M.J. 545 (A.C.C.A. 2011).

"Special findings are to a bench trial as instructions are to a trial before members. Such procedure is designed to preserve for appeal questions of law. *Cesario v.*

*United States*, 200 F.2d 232, 233 (1st Cir. 1952). It is also the remedy designed to rectify judicial misconceptions regarding: the significance of a particular fact, *Wilson v. United States*, 250 F.2d 312, 325 (9th Cir. 1958); the application of any presumption, *Howard v. United States*, 423 F.2d 1102, 1104 (9th Cir. 1970); or the appropriate legal standard, *United States v. Morris*, 263 F.2d 594 (7th Cir. 1959)."

*United States v. Truss*, 70 M.J. 545 (A.C.C.A. 2011), quoting *United States v. Falin*, 43 C.M.R. 702 (A.C.M.R. 1971).

4. The Court should follow one of the suggested formats prescribed in Appendix F of the Department of the Army Pamphlet 27-9 to enter its special findings.

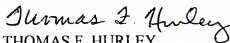
#### CONCLUSION

5. The Defense requests this Court to enter special findings for each of the specifications and charges as requested above.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel



THOMAS F. HURLEY  
MAJ, JA  
Defense Counsel



JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

Prosecution Notification  
to the Court:  
GAL Evidence

19 July 2013

On 18 July 2013, the Court ordered the United States to set forth admitted evidence related to a user's authorization to download or remove information from the United States Forces-Iraq Microsoft Outlook/SharePoint Exchange Server global address list (hereinafter "GAL"). In accordance with the Court's order, the United States proffers the following.

Army Regulation 25-2 (hereinafter "AR 25-2") defines an information system as a "[s]et of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information." Prosecution Exhibit (hereinafter "PE") 93 at 86-87.<sup>1</sup> AR 25-2 adds that this "includes [Army Information System] applications, enclaves, outsourced IT-based processes, and platform IT interconnections." *Id.* The GAL collects, stores, and processes military information. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard. The GAL is an information system under AR 25-2.

AR 25-2 prohibits Soldiers from using an employee-owned information system for classified or sensitive information. PE 93 at 47 (citing AR 25-2 ¶ 4-31(a)). Furthermore, "[t]he use of an [employee-owned information system] for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with [Information Assurance Manager], [Designated Approving Authority], or commander approval." *Id.* (citing AR 25-2 ¶ 4-31(b)). COL Miller testified that the accused was not authorized to engage in the charged misconduct, to include the asportation of records and United States government information to WikiLeaks. *See* Testimony of COL Miller.

AR 25-2 defines sensitive information as "[a]ny information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552(a) (The Privacy Act). . . ." PE 93 at 21 (citing AR 25-2 ¶ 4-4(b)(2)) (emphasis added); PE 93 at 98 (citing AR 25-2 definition of sensitive information); *see also* AR 530-1 ¶ 1-5(c) (defining sensitive information to include, *inter alia* information related to names, unit assignment, or organizations); AR 530-1 ¶ 2-1 (stating that Soldiers will protect from disclosure sensitive information to which they have access). Sensitive information includes, *inter alia*, "information in routine DOD payroll, finances, logistics, and personnel management systems." PE 93 at 92. This list is non-exhaustive. *See id.* AR 25-2 also mandates that "[a]ll Army personnel" will "protect and restrict access to all documentation . . . describing IS architectures,

<sup>1</sup> PE 93 is a copy of AR 25-2. The page numbers cited in this filing correspond to the page numbers printed in AR 25-2, not the electronic page numbers of the .pdf.

designs, configurations, vulnerabilities, address listings, or user information.” PE 93 at 38 (citing AR 25-2 ¶ 4-13(a)).

The loss or misuse of the information in the GAL could affect or harm the privacy of listed Servicemembers. *See* Testimony of CW4 Nixon. The GAL contained personally identifiable information. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard; Testimony of Mr. Lewis. The GAL operates as a “phonebook” for a user. *See* Testimony of CW4 Nixon. The GAL identified, *inter alia*, a user’s name, username, domain, alias addresses, certificates, unit, and phone numbers. *Id.*; *see* PE 47; PE 48; PE 147(a); PE 148(b). This information also revealed organizational structure. *See* Testimony of CW4 Rouillard. The GAL and its contents were not available to the public and were available only to authorized personnel. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard. In 2010, a user did not have the capability to export the GAL from the server onto an authorized NIPR computer. Testimony of CW4 Nixon.

The loss or misuse of the information in the GAL could affect or harm military operations and system security. *See* Testimony of CW4 Rouillard; Testimony of CW4 Nixon. Adversarial forces value and seek the GAL and its contents. *See* Testimony of CW4 Rouillard; Testimony of Mr. Lewis. The GAL reveals user names, which increases the ability of a malicious actor to compromise United States computer systems. *See* Testimony of CW4 Rouillard. Accordingly, a malicious actor could use the GAL for spear phishing attacks to compromise United States computer systems. *Id.* The GAL further reveals network architecture, *see* Testimony of CW4 Rouillard, thereby aiding an adversary’s offensive operations against United States computer systems. *See* PE 93 at 38 (citing AR 25-2 ¶ 4-13(a)); *see also* PE 93 at 22 (citing AR 25-2 ¶ 3-3(c)(5) (mandating protection of system and network integrity)). Additionally, the GAL could be used as part of a social engineering attack against Soldiers. *See* Testimony of CW4 Rouillard. Thus, the information in the GAL was sensitive and protected under AR 25-2 ¶ 4-31(a).

The accused’s commander did not authorize the exfiltration of the GAL. *See* Testimony of COL Miller. Moreover, AR 25-2 prohibits downloading the GAL to a NIPR computer and moving it to a personal computer. *See* Testimony of CW4 Rouillard (stating that AR 25-2 prohibits downloading the GAL to a personal computer and that the ability to do an act on a computer system does not mean the act is authorized); PE 93, *supra*. The accused had no reason to download the GAL to his personal computer because he could only send emails from his NIPR computer. *See* Testimony of CW4 Nixon. Therefore, AR 25-2’s prohibition on using a personal computer for sensitive information applied to the GAL and its contents. *See* PE 93, *supra*; *cf.* AR 25-1 ¶ 6-1(d)(1) (4 December 2008) (limiting use of United States Government systems “to the conduct of official business or another authorized use”); PE 93 at 22 (citing AR 25-2 ¶ 3-3(c)(4)-(5) (stating that users must protect information systems located in their respective areas and take no actions that “threaten the integrity of the system or network”)); PE 93 at 28 (citing AR 25-2 ¶ 4-5(a)(7) (prohibiting transfer or possession of information without proper authority)).

In the time period when the accused extracted the GAL, WikiLeaks published a tweet requesting “.mil email addresses.” PE 31. Extracts of 74,000 email accounts from the GAL

were found on the accused's computer. See Testimony of Special Agent Williamson; Testimony of Special Agent Johnson; Testimony of CW4 Nixon (identifying Servicemember names and email accounts in PE 47 and PE 48 as originating from the GAL). The accused created a tasker to describe his mission to "acquire and exfiltrate" the GAL. The accused's tasker defines the purpose as "[t]o e-mail classified messages from USF-1's CIDNE event log from 2004 to 2009." This purpose suggests the tasker was used for previous compromises of sensitive information and that accused's mission regarding the GAL was conducted with the same intent. Consequently, where AR 25-2 prohibited the accused from placing the sensitive information on his personal computer, the accused completed his crime when he completed the prohibited act with a criminal intent.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail, on 19 July 2013.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**SUPPLEMENTAL RULING:  
Defense Motions For Findings of Not  
Guilty - RCM 917**

24 July 2013

This ruling supplements the Court's 18 July 2013 ruling and addresses the Defense motions under RCM 917 for findings of not guilty for specifications 4, 6, 8, 12, and 16 of Charge II (Stealing, Purloining, or Knowingly Converting (SPKC) Records or Things of Value Belonging to the United States, in violation of 18 U.S.C. §641 and Article 134, UCMJ).

**Defense Position:** The Defense moves the Court to enter a finding of not guilty in accordance with RCM 917 because:

1. In each of the specifications 4, 6, 8, 12, and 16, the Government charged the accused with SPKC the actual databases themselves and did not allege in the charge that the accused SPKC the records in the database, or a copy of the records in the database, or the information in the records. This is a fatal variance between what is charged and the evidence presented.
2. Even if properly charged, intangible property, such as information, is not within the scope of 18 U.S.C. §641.
3. The Government has not proved substantial or serious interference with the Government's use and benefit of the charged databases. The databases, records, and information remained available for the Government's use without change after the alleged SPKC by the accused.
4. The Government has failed to adduce any value of copies or information. Should the Court find that specifications 4, 6, 8, 12, and 16 properly charge SPKC of records, copies of records, or information, the Government has failed to adduce evidence of the value of the records, copies, or the information contained therein.
5. For specification 16 of Charge II, the Defense further alleges that the Government has failed to present evidence that the .mil addresses found on the accused's personal Macintosh (MAC) computer were the U.S. Forces - Iraq Microsoft Outlook/SharePoint Exchange Server global address list (USF-I GAL). The Defense further alleges that even if the accused downloaded a GAL, the Government has failed to introduce evidence that he acted "with intent to deprive the government of the use and benefit of the records" that the accused's conduct was wrongful, or that the accused's conversion of the GAL caused serious or substantial interference with the Government's ownership rights as the GAL was available for use with no change after the accused allegedly converted it.



**Government Position:** The Government opposes the Defense motion arguing that:

1. Specifications 4, 6, 8, 12, and 16 of Charge II each identify the records in the relevant database that the accused is charged with SPKC. Information is inherent within the definition of record and database. Thus, there is no fatal variance between pleading and proof.
2. The contents and information contained in Government records determine the criminality of the SPKC of the records more than the form of the records.
3. For conversion purposes, the deprivation of the Government's right to protect the contents of confidential classified information can be a misuse that seriously and substantially interferes with the Government's property rights.
4. The Government provided evidence of value in excess of \$1,000.00 for specifications 4, 6, 8, 12, and 16 through the testimony of Mr. Lewis, by evidence of the cost of creating the records at issue, and the costs of creating and maintaining the databases at issue via the database management systems, infrastructure, and software. The cost of the database management infrastructure is appropriate evidence of value because without it, the records would not exist and could not be downloaded.
5. With respect to specification 16 of Charge II, the Government argues that evidence presented by the Government that the accused created a tasker to "exfiltrate" the GAL after receiving a 7 May 2010 tweet from WikiLeaks seeking .mil addresses, that the accused extracted the 74,000 addresses from the USF-I GAL and placed the extracted information on his personal MAC computer, together with evidence of his history of downloading classified government records and information, transferring it to personal digital media, and sending the records and information to WikiLeaks and testimony from CW4 Nixon that the USF-I GAL contained names and email addresses connected to the "iraq.centcom.mil" domain establish that the 74,000 email addresses came from the USF-I GAL pool and that the GAL contains usernames, domains, alias addresses, certificates, unit, and phone numbers and reveals unit organizations structure, information defined as "sensitive" per Army Regulations (AR) 25-2 and 530-1 establishes that the accused SPKC the USF-I GAL from the possession of the United States with intent to deprive the United States of the stolen property and that his conduct was wrongful.
6. In part B (1-5) of its brief (AE 599), the Government identified the evidence admitted to prove each of the elements for specifications 4, 6, 8, 12, and 16 of Charge II. The Court has reviewed all of the testimony and examined the evidence set forth by the Government for each specification as well as the briefs and oral argument presented by the parties.

**Oral Argument:** On 18 July 2013, the Court heard oral argument on this motion and received AE 610, a Property/Value of Property Chart from the Defense. On 19 July 2013, the Court received Prosecution Notification to the Court: GAL Evidence (AE 612). On 20 July 2013, the Court held additional oral argument. During this oral argument, the Government conceded that the evidence for specifications 4 and 6 of Charge II shows that the CIDNE-I and A sigacts the accused is charged with SPKC comprised approximately 25% of the CIDNE-I and A databases. The Government also advised the Court that for specification 16 of Charge II, the Government

was going forward only with the 74,000 addresses allegedly downloaded by the accused rather than charging the accused with SPKC the email addresses of all 160,000 users on the USF-1 GAL. The Government moved to amend specifications 4, 6, and 16 of Charge II to except "to wit:" and substitute "to: wit, a portion of" for each specification. The Government further moved the Court to allow evidence of a pro rata share of the database management costs for each specification. The Defense opposed the amendments as major changes under RCM 603(d) and moved the Court for a mistrial under RCM 915 with respect to specifications 4, 6, and 16 because the Defense had no opportunity to cross examine the valuation witnesses with respect to pro rata share. The Defense argues a mistrial is manifestly necessary in the interest of justice because the Government's action to amend specifications 4, 6, and 16 of Charge II after presentation of the evidence on the merits casts substantial doubt over the fairness of the proceedings.

### **Findings of Fact:**

1. Specifications 4, 6, 8, 12, and 16 of Charge II all have the same charging structure:

In that Private First Class Bradley E. Manning, U.S. Army, did, at or near Contingency Operating Station Hammer, Iraq, between on or about [applicable dates], steal, purloin, or knowingly convert to his use or the use of another, a record or thing of value of the United States or of a department or agency thereof, to wit:

Specification 4: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records;

Specification 6: the Combined Information Network Exchange Afghanistan database containing more than 90,000 records;

Specification 8: a United States Southern Command database containing more than 700 records;

Specification 12: the Department of State Net-Centric Diplomacy database containing more than 250,000 records;

Specification 16: the United States Forces – Iraq Microsoft Outlook/SharePoint Exchange Server global address list;

of a value of more than \$1,000, in violation of 18 U.S. Code Section 641, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

2. Relevant instructions the Court will give for the 18 U.S.C. §641 offenses are:

To "steal" means to wrongfully take money or property belonging to the United States government with the intent to deprive the owner of the use and benefit temporarily or permanently.

"Wrongful" means without legal justification or excuse.

To “purloin” is to steal with the element of stealth, that is, to take by stealth the property of the United States government with intent to deprive the owner of the use and benefit of the property temporarily or permanently.

A “taking” doesn’t have to be any particular type of movement or carrying away. Any appreciable and intentional change in the property’s location is a taking, even if the property isn’t removed from the owner’s premises. The accused did not have to know the United States government owned the property at the time of the taking.

A “conversion” may be consummated without any intent to permanently deprive the United States of the use and benefit of the property and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include the misuse or abuse of property. It may reach use in an unauthorized manner or to an unauthorized extent of property placed in one’s custody for limited use. Not all misuse of government property is a conversion. The misuse must seriously and substantially interfere with the United States government’s property rights.

“Value” means the greater of (1) the face, par, or market value, or (2) the price, whether wholesale or retail. A “thing of value” can be tangible or intangible property. Government information, although intangible is a species of property and a thing of value.

The market value of stolen goods may be determined by reference to a price that is commanded in the market place whether that market place is legal or illegal. In other words, market value is measured by the price a willing buyer will pay a willing seller. (The illegal market place is also known as a “thieves market”). “Cost price” means the cost of producing or creating the specific property allegedly stolen, purloined, or knowingly converted.

4. The “thieves market” may be used to establish value so long as the Government presents evidence of the value of the property or information at issue in the “thieves market”. *U.S. v. Hood*, 12 M.J. 890 (A.C.M.R. 1982); *U.S. v. Oberhardt*, 887 F.2d 790 (7<sup>th</sup> Cir. 1989).

5. The Court takes judicial notice that Black’s Law Dictionary (9<sup>th</sup> ed. 2009) defines a database in relevant part as “a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means.” The Court takes judicial notice that Black’s Law Dictionary defines a record as “information that is inscribed on a tangible medium or that, having been stored in an electronic or other medium, is retrievable in perceivable form.” Databases are supported by database management systems, infrastructure, and software.

6. The records the accused is charged with SPKC in specifications 4, 6, 8, 12, and 16 of Charge II are maintained on classified electronic databases. The databases, records, and information contained therein, are accessible only to individuals with security clearances who have been approved by the Government to have access to the information. The structure of the databases allows multiple authorized users to access and extract the information maintained on the database simultaneously. The records in the database, and the information contained therein,

may be extracted or downloaded from the database by authorized users, however, the records, and information therein, remain in the database after extraction by user(s) in the same condition as they existed prior to the extraction.

7. Specification 16 of Charge II, charges the accused with SPKC the USF-I GAL. The evidence presented by the Government provides some evidence that 74,000 .mil addresses were found on the NIPR supply room computer in the peter.bigelow account and on the accused's personal MAC computer.

8. On 16 February 2012, the Defense filed a motion for a bill of particulars. In paragraph 10(a) and (b), the Defense asked the following with respect to the specifications charging a violation of 18 U.S.C. §641: (1) What specific theory of culpability does the government intend to rely upon? In other words, does the Government allege that PFC Manning "stole", "purloined" or "converted"? and (2) If the Government is alleging that PFC Manning stole, purloined, and converted the charged items, does each theory of culpability apply equally to every charged item? On 8 March 2012, the Government responded to paragraph 10(a) and (b) of the Defense request for a bill of particulars with a paragraph arguing that it should not be directed to submit a bill of particulars because the Defense was attempting to restrict the Government's proof at trial. In the paragraph the Government included the following sentence "Furthermore, the theft-related offenses alleged in this case are of specific, identified databases." In the bill of particulars, the Defense posed questions with regard to the Government's theory of prosecution. The Defense did not seek more specificity as to the items charged. Nor did the Defense seek clarification after receiving the Government's response. The Court finds the language of the specifications themselves, rather than the Government's bill of particulars, response provides the accused notice of what the accused is charged with SPKC.

### Conclusions of Law:

1. 18 U.S.C. §641 was intended to encompass all forms of common law larceny. *Morrisette v. United States*, 342 U.S. 246, 253 (1952). The statute encompasses SPKC of intangible information. Intangible information is "a thing of value" under 18 U.S.C. §641. *U.S. v. Matzkin*, 14 F.3d 1014 (4<sup>th</sup> Cir. 1994); *U.S. v. Lambert*, 446 F.Supp. 890 (D.C. Conn. 1978), *aff'd United States v. Girard*, 601 F.2d 69, 70 (2<sup>nd</sup> Cir. 1979); *U.S. v. Collins*, 56 F.3d 1416, 1420 and n. 3 (D.C. Cir. 1995) (While not central to our analysis, we note that every circuit, except one, dealing with this issue has held that intangible property falls within the purview of §641.). See e.g. *United States v. Jeter*, 775 F.2d 670, 680 (6<sup>th</sup> Cir. 1985) ("the Congress' very use of the more expansive 'thing of value' rather than 'property' strongly implies coverage beyond mere tangible entities."), *cert. denied*, 475 U.S. 1142 ... (1986); *United States v. Croft*, 750 F.2d 1354, 1361 (7<sup>th</sup> Cir. 1984) (services rendered constitute a thing of value); *United States v. May*, 625 F.2d 186, 191-92 (thing of value includes flight time); *United States v. Girard*, 601 F.2d 69, 71 (2<sup>nd</sup> Cir. 1979) (content of a writing, while an intangible, is a thing of value), *cert. denied* 444 U.S. 871...(1979). [Note 3] The Ninth Circuit in *Chappell v. United States*, 270 F.2d 274 (1959), held conversion was limited to tangible chattels under §641. This holding, however, remains in doubt within the Circuit itself. See *United States v. Schwartz*, 785 F.2d 673, 681 n. 4 (9<sup>th</sup> Cir. 1986) ("this court has not cited *Chappell* in support of its limited interpretation of *thing of value* since that case was decided in 1959"). Even if SPKC intangible information included

in a SPKC of tangible information was not an offense under 18 U.S.C. §641, it would constitute an offense as charged in specifications 4, 6, 8, 12, and 16 under clauses one and two of Article 134, UCMJ.

2. Specifications 4, 6, 8, and 12 of Charge II, charge the accused with SPKC a specified database and a number of records contained within that database. Information is necessarily included within the definition of both record and database. Thus, specifications 4, 6, 8, and 12 of Charge II provide the accused notice that he is accused of stealing the information in the described records and databases described in the specifications and protect him from another prosecution for the same conduct. There is no material or fatal variance between the pleadings and the proof.

3. In specification 16 of Charge II, the accused is charged with SPKC the USF-I GAL. The fact that there were fewer email addresses found on the accused's computer than included in the USF-I GAL is not a material variance. The evidence presented by the Government provided some evidence to show that the USF-I GAL was produced by incorporating user data from the bottom up (brigade to division to USF-I) with the domain *iraq.centcom.mil*. Thus, a subset of the USF-I GAL, would be a lesser included offense for the fact-finder. There is no material or fatal variance between the pleading and the proof.

4. The Government has moved to amend specifications 4, 6, and 16 to conform with the evidence that the records, and information therein, allegedly SPKC by the accused were portions of the databases alleged to have been SPKC by the accused. The amendments proposed by the Government do not change the nature of the offenses, add a party, offense, or substantial matter not fairly included in the original specifications. The proposed amendments do not mislead the accused. The amendments make the offenses lesser included offenses of the original specifications. They are minor changes under RCM 603(a). The Court grants the Government's motion to amend specifications 4, 6, and 16 to except the words "to wit" and substitute the words "to wit: a portion of".

5. A stealing or purloining requires that the accused wrongfully take money or property belonging to the United States with the intent to deprive the owner of the use and benefit temporarily or permanently. The Government does not have to prove that the Government suffered a loss or was deprived of the use and benefit of the records, databases, or information therein, to prove a stealing or purloining for the 18 U.S.C. §641 specifications. The fact that the Government sustains no loss or actually receives some service or benefit as a result of the accused's action does not negate the accused's criminal intent. *U.S. v. Ayesh*, 702 F.3d 162, 169 n. 2 (4<sup>th</sup> Cir. 2012) (Indeed at least four circuits – the First, Fifth, Seventh, and D.C. Circuits – have found that the Government need not prove an actual loss to establish a violation of §641. *See United States v. Herrera-Martin*, 525 F.3d 60, 62, 64 (1<sup>st</sup> Cir. 2008) (affirming the conviction of a defendant who used another person's name and identifying information to obtain a federal housing voucher); *United States v. Milton*, 8 F.3d 39, 41, 44 (D.C. Cir. 1993) (affirming the convictions of two brothers who helped others submit false claims for back pay under a settlement agreement between an employer and the Equal Employment Opportunity Commission); *United States v. Barnes*, 761 F.2d 1026, 1027-28, 133 (5<sup>th</sup> Cir. 1985) (affirming the convictions of two defendants who applied for and authorized fraudulent livestock loans

from the Farmers Home Administration, even though the money had actually been used to buy livestock); *United States v. Bailey*, 734 F.2d 296, 298-301 (7<sup>th</sup> Cir. 1984) (affirming the conviction of a defendant attorney who had embezzled portions of loans used by the Farmer's Home Administration). *But see United States v. Collins*, 464 F.2d 1163, 1164-65 (9<sup>th</sup> Cir. 1972) (reversing a conviction under §641 after finding that the money that the defendant had stolen by forging and negotiating government-issued checks had belonged to a bank not the government)).

6. A "conversion" may be consummated without any intent to permanently deprive the government of the use and benefit of the property and without any wrongful taking. Not all misuse of government property is a conversion. The misuse must seriously and substantially interfere with the government's property rights. *Collins*, 464 F.2d at 1420; *U.S. v. May*, 625 F.2d 186, 192 (8<sup>th</sup> Cir. 1980) *quoting Restatement (Second) of Torts* §222A (One who is authorized to make a particular use of a chattel, and uses it in a manner exceeding the authorization, is subject to liability for conversion to another whose right to control the use of the chattel is thereby seriously violated.).

7. In this case, the Government elicited evidence that the Government maintained exclusive possession and stringent controls over the classified information, records, and databases charged in specifications 4, 6, 8, and 12 of Charge II. The Government authorized access to the information and records only by individuals to whom the Government had given appropriate security clearances. The Government maintained possession of the information and records on classified SIPR computers. The Government provided further evidence that the accused extracted and removed the classified records, and information therein, from the SIPR computer in the 2<sup>nd</sup> Brigade (Bde) Sensitive Compartmented Information Facility (SCIF), downloaded them to his own portable digital media or platform, removed the portable digital media and platform from the 2<sup>nd</sup> Bde SCIF, transferred the records, and information therein, to his personal portable digital media or platform in his private housing unit, and then transferred the records, and information therein, to WikiLeaks. The Court finds this to be some evidence of a misuse of Government records that could seriously and substantially interfere with the Government's property right to control the charged records, and information therein, to withstand a motion for a finding of not guilty under RCM 917. For specification 16 of Charge II, the Government is not pursuing a theory of conversion.

8. SPKC of electronic data doesn't compare neatly to cases where the defendant made photocopies of government records, replaced the originals, and SPKC the photocopies. With SPKC, there are no copies to steal until the accused accesses the digital information and makes the extraction. The original digital database and records remain in the database management system during and after extraction.

9. The Government has not charged the accused with SPKC a copy of Government records in the 18 U.S.C. §641 specifications. The Government is charging the accused with stealing and purloining the databases, electronic records, and information therein, at issue by accessing the relevant database, extracting the records from the database management system structure, placing the information on private platforms or digital media while in the 2<sup>nd</sup> Bde SCIF at Forward Operating Base (FOB) Hammer, and asporting the downloaded records, and information contained therein, to the accused's personal platforms or digital media outside the

SCIF in his housing unit. The Government's theory is that the accused knowingly converted the records, and information therein, in specifications 4, 6, 8, and 12 by sending them to WikiLeaks.

10. The value of the information the accused is alleged to have SPKC in specifications 4, 6, 8, 12, and 16 may be considered to determine whether the value of the charged database, records, or information therein, is over \$1,000.00. That said, the accused is not charged in specifications 4, 6, 8, 12, or 16 of Charge II with SPKC any of the database management systems, infrastructure, or software. As amended, the accused is not charged with SPKC the entire databases in specifications 4, 6, and 16 of Charge II.

11. The Government argues that the databases, records, and information in these specifications would not exist without the database management system, infrastructure, and software. The Government proposes the value of the cost of creating and maintaining the database management system, infrastructure, and software as a basis to value of the databases, records, and information therein, for specifications 8 and 12 of Charge II. The Government further proposes to establish the value for the records, and information contained therein, by establishing the value of a pro rata share of the cost of creating and maintaining the database management system, infrastructure, and software for the databases in specifications 4, 6, and 16 of Charge II. A similar argument could have been advanced in *U.S. v. May*, 625 F.2d 186 (8<sup>th</sup> Cir. 1980) to allow the Government to value the converted flight time by valuing the cost and maintenance of the airplane itself, because the converted flight time couldn't exist without the existence of the airplane. The Government has proffered no authority where a court has allowed the Government to equate the value of a database, records in a database, or information therein, SPKC by an accused or defendant with the value of the cost of creating and maintaining the database management system, infrastructure, or software. This is a case of first impression in the volume of database records, and information therein, alleged to have been SPKC by an accused or defendant. If the accused downloaded 10 records from one of the databases alleged in the 18 U.S.C. §641 specifications, the 10 records would also not exist without the database management infrastructure, system, and software. The Government's proffer for relying on the value of the cost of creating and maintaining the database management system, infrastructure, and software to establish value of the databases, records, and information contained therein, relies on the volume of records allegedly SPKC by the accused. The Court further recognizes that the Government's amendments to specifications 4, 6, and 16 of Charge II after the presentation of the evidence to allege portions of the databases and USF-I GAL does not afford the Defense the opportunity to cross examine any of the valuation witnesses on the pro rata share of the databases or USF-I GAL or to present evidence regarding the pro rata share of the databases or USF-I GAL.

12. The Government may not base the value of the database, records, or information therein, for specifications 4, 6, 8, 12, and 16 of Charge II on the value of the cost of creating and maintaining the database management system, infrastructure, or software. The Court will disregard all evidence presented of such value when acting as the fact-finder. The Government may present and argue thieves market evidence regarding the value of the database, records, and information therein, and on cost production evidence presented regarding the cost of creating the information in the charged databases and records, such as employee time and salary for data entry.



13. The Court reaffirms its 2 July 2013 ruling at AE 591 (Government Motion to Qualify Mr. Daniel Lewis as an Expert). The evidence presented by the Government of value in the thieves market in excess of \$1000 for the records, and information contained therein, for specifications 4, 6, 8, 12, and 16 of Charge II is some evidence of value under RCM 917(d) to withstand a motion for a finding of not guilty.

14. The Court's ruling mitigates any prejudice to the accused resulting from the Government's amendments to specifications 4, 6, and 16 of Charge II. The Defense motion for a mistrial as to those specifications is denied.

15. The Court has examined the testimony and evidence identified by the Government in part B(1-5) of its brief (AE 599) admitted to prove each of the elements for specifications 4, 6, 8, 12, and 16 of Charge II. The evidence presented by the Government, together with all reasonable inferences and applicable presumptions, viewed in the light most favorable to the Government, without an evaluation of the credibility of the witnesses, could reasonably tend to establish every essential element of specifications 4, 6, 8, 12, and 16 of Charge II.

**Ruling:**

1. The Defense Motions for a Finding of Not Guilty for specifications 4, 6, 8, 12, and 16 of Charge II is **DENIED**.
2. The Government motion to amend specifications 4, 6, and 16 of Charge II is **GRANTED**.
3. The Defense Motion for Mistrial is **DENIED**
4. The Government may not base the value of the charged databases, records, or information therein, on the value of creating or maintaining the database management system, infrastructure, or software. The Court will disregard such evidence presented as the fact-finder. The Government will not refer to such evidence in closing argument.

So **Ordered** this 24th day of July 2013.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit



IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION FOR  
RECONSIDERATION AND FOR  
MISTRIAL: SPECIFICATIONS  
4, 6, 8, 12, 16 OF CHARGE II  
(18 U.S.C. §641 OFFENSES)**

DATED: 24 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 905(f), requests that this Court reconsider its Supplemental Ruling on Defense Motions for Findings of Not Guilty dated 24 July 2013 ("Ruling") and declare a mistrial as to all the 18 U.S.C. Section 641 offenses. The Defense submits that the Government has made an utter mess of the section 641 offenses by pursuing one charge (that PFC Manning stole databases) and at the last-minute pursuing a different charge (that PFC Manning stole information). The Defense did not know that "database" or "records" meant "information" and has suffered irreparable prejudice as a result.

STANDARD

2. Under R.C.M. 915, a military judge may declare a mistrial when "manifestly necessary in the interest of justice because of circumstances arising during the proceedings which cast substantial doubt upon the fairness of the proceedings."

EVIDENCE

3. The Defense requests that you consider the Attachment (Affidavit from Mr. Cassius Hall). The Defense also requests that the Court consider the evidence adduced by the Government during the merits phase of the trial.

ARGUMENT

**A. The Defense Did Not Know that Either "Databases" or "Records" Included "Information" until 24 July 2013, After the Close of Evidence**

4. The Court has ruled that the word "databases" includes the records and information contained in the databases, pointing to the definition of "database" in Black's Law Dictionary. The Court states that "information is necessarily included within the definition of both records or databases." See Ruling p. 6. The Court does not provide any authority for this conclusion of law and the Defense does not believe that this conclusion of law can be reconciled with the Charge Sheet and the presentation of evidence in this case. Nor can it be reconciled with federal case law. See Defense R.C.M. 917 Motions.

*i. "Information" is Not Necessarily Included in the Definition of "Databases" Based on the Use of The Term "Databases" In This Case*

5. The Court has accepted the Government's argument that databases = records = information. If this were the case, how difficult would it have been for the Government to actually charge "information" in the Charge Sheet? Why did it use the word "database"? Why are we in a position, three years into the case and after the presentation of all the evidence, where we have to read one word ("information") into another word ("database" or "records")? Why is it that the Defense is the party that is penalized for an apparent misunderstanding of the charged property? Why is the Government not held to task for using one word ("database") when it apparently meant another ("information")?

6. If one thing should be clear in a Charge, it is the property that is alleged to have been stolen or converted. Why is an ambiguity in the Charge placed at the feet of the Defense, rather than the Government? The fact that the Court needed to look to Black's Law Dictionary, the parties submitted approximately 50 pages of motions on the topic, the Court heard multiple oral arguments on the issue, and the Court took over a week to decide the motion, all suggest that the issue is not as clear as the Court now makes it seem. If it were apparent to everyone that database = information, why the need for protracted litigation over the issue?

7. Moreover, even though Black's Law Dictionary defines database as it does, there are other logical understandings of the word "database." The Government charged that PFC Manning stole a database containing X number of records. If database = records = information, then the charge would have referred to PFC Manning stealing "a database of X number of records." In other words, the Government's charging of database containing X number of records suggest that the database refers to the receptacle for the information or records. Furthermore, although the Court was apparently not persuaded by this argument, one could easily have an empty database (i.e. one that does not contain records or information). For instance, we heard testimony that the State Department contracted with an outside agency to create the Net-Centric Diplomacy database. See Mr. Charlie Wisecarver. Presumably, when it contracted with this outside agency, it was to create the receptacle for the various cables that were added later. Further, various witnesses testified that the specific databases were "systems" or "programs" and did not indicate that the database was coextensive with its informational content. See Mr. Wyatt Bora ("CIDNE is a reporting and querying system."). The point of this is to illustrate that there are different, and equally reasonable, understandings of the word "database." Simply because the Court prefers one interpretation over another does not mean that the Defense was on notice of the interpretation that the Government has now urged the Court to accept and that the Court has apparently accepted.

8. The Government itself sought to prove that PFC Manning stole “databases” (i.e. the receptacle or infrastructure associated with maintaining the records). Approximately 95% of its valuation evidence took the form of proving the value of the databases, not the information or the records. This shows that the Government itself, when it used the word “databases” in the Charge Sheet meant databases, not information or records. The Defense, seeing all the evidence that the Government was adducing on the database, was eminently reasonable in assuming that when the Government charged “database” it meant “database” (the physical receptacle for the information).<sup>1</sup>

9. Even the definition accepted by the Court presupposes that a database is *more* than simply the information it contains. The definition relied on by the Court refers to a database as “a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means.” Ruling at p. 4. Even under this definition, a database contains elements other than information—it includes the organizational structure (“arranged in a systematic way”) and search capabilities (“offering a means of finding specific elements it contains”). These are necessarily included in the concept of database (indeed, they are what distinguishes a “database” from “data”). And now the Court has concluded that the Government does not need to actually prove what the Government charged—the entire database, to include elements other than information. This fundamentally changes the nature of the offense and irreparably prejudices the accused.

*ii. Federal Case Law Definitively Establishes that “Information” is Not Included in “Records”*

10. Federal case law definitively establishes that “information” is not necessarily embraced within the concept of “records” within the meaning of section 641 for the following reasons:

- a) One federal circuit, the Ninth Circuit, does not accept that information can fall within section 641. See *United States v. Chappell*, 270 F.2d 274, 277 (9th Cir. 1959); *United States v. Tobias*, 836 F.2d 449 (9th Cir. 1988). Accordingly, information cannot ever be a “record” within the meaning of section 641 under this circuit’s interpretation. Another federal circuit has expressed reservation over using section 641 to charge information. See *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). Given these courts’ interpretation of information, it cannot be said that the word “records” necessarily encompasses information.
- b) Federal courts that have accepted that section 641 applies to information have uniformly held that information falls within the “thing of value” prong of section 641, not the “records” prong of section 641. See *United States v. DiGilio*, 538 F.2d 972, 978, fn 10 (3rd Cir. 1976) (“The government obviously did not consider this merely a theft of information case, because the indictment charges defendants only with converting to their use government records. Section 641 also prohibits conversion of any ‘thing of value’, and the government would presumably rely on this term in an information case”); *United*

<sup>1</sup> The Defense also believes that the word database can refer to the combination of the “receptacle” and its records, but it cannot refer to the records alone. The Defense does not believe that database can fairly be read to include information for the reasons identified herein, and for the reason that databases do not always contain information (e.g. one may have a database of videos, music, photographs, etc.).

*States v. Jordan*, 582 F.3d 1239, 1246 (11th Cir. 2009) (indictment under §641 alleged that defendant's "delivered the printouts which as property of the United States had a value in excess of \$1000"; in a separate count, indictment alleged that defendant received "a thing of value of the United States, that is, information contained in the NCIC records."); *United States v. Girard*, 601 F.2d 69, 71 (D. Conn. 1979) ("we are impressed by Congress' repeated use of the phrase "thing of value" in section 641 and its predecessors. ... The word "thing" notwithstanding, the phrase is generally construed to cover intangibles as well as tangibles. ... Although the content of a writing is an intangible, it is nonetheless a thing of value"). If this is the case—i.e. information and records are two different things under section 641—then how can "information" be fairly encapsulated within the concept of records?

- c) All federal case law where "information" was alleged to have been stolen actually alleged *in the charge sheet* that information was stolen. See e.g. *United States v. Jeter*, 775 F.2d 670, \*680-1 (6<sup>th</sup> Cir. 1985) ("The government charged that Jeter 'did willfully and knowingly embezzle, steal, purloin and convert to his own use and the use of others, and without authority did sell, convey and dispose of records and things of value of the United States, the value of which is in excess of \$100.00, to wit, carbon paper and the information contained therein relating to matters occurring on October 5, 1983, before a grand jury'"); *United States v. DiGilio*, 538 F.2d 972 (3<sup>rd</sup> 1976) (government charged that the defendants converted to their own use "records of the United States; that is, photocopies of official files of the Federal Bureau of Investigation"); *United States v. Jordan*, 582 F.3d 1239, 1246 (11th Cir. 2009) (indictment under §641 alleged that defendant's "delivered the printouts which as property of the United States had a value in excess of \$1000"; in a separate count, indictment alleged that defendant received "a thing of value of the United States, that is, information contained in the NCIC records."). Federal case law does not rely on reading into a word like "database" or "record" the concept of information.

The Defense, and the accused, should not be penalized for being aware of federal case law on section 641. As the Defense argued in its motion to dismiss, *every* federal case where the theft of information was alleged *actually charged* theft of information. The Court failed to reference this fact in its Ruling, apparently believing that such a factor was unimportant to its disposition. However, such a factor is critical—since this will be the only prosecution to be maintained based on theft of "information" where "information" was not actually charged. A federal accused should not fare better than a military accused in terms of the notice provided to him under federal law (i.e. a federal accused's Charge Sheet will state that the accused stole "information", while a military accused must extrapolate "information" from the word "database"). If the Government chooses to incorporate federal law, then federal law in terms of charging and proving the offense, must be followed.

11. The Court also failed to reference the cases cited by the Defense (*United States v. Marshall*, No. 08-0779 (C.A.A.F. 2009) and *United States v. Veloria*, 2011 WL 1330779) that indicate the importance of the charging decision in terms of what it provides notice of. This is presumably because these cases involved variances, whereas this Court believes that no variance is required because the specification put the accused on notice of the charges. However, in those cases, the difference between the charges and proof was arguably less significant than it is here. Here, the

*very property* at issue is subject to dispute. This is, in the Defense's view, more critical than who the accused allegedly escaped from, or who the money technically belonged to. If those cases concluded that there was a fatal variance between pleadings and proof, so too should have been the case here. The Government never did establish that PFC Manning stole "databases" – whether one defines databases as the receptacle alone, or the receptacle plus the records in that receptacle. And now the Court has given the Government a get-out-of-jail free card by allowing the Government to avoid the necessity of proving the value of the receptacle, even though the Government itself embarked on a mission to prove the value of the receptacle. In short, not even the Government knew what it was proving when it charged and pursued the section 641 offense.

**B. The Defense Has Been Irreparably Prejudiced by the After-the-Close-of-Evidence Ruling that Databases = Information**

12. Based on the Defense's knowledge of section 641 case law, the Government's insistence that it was proving theft of "databases", the Government's proffer in its Instructions that it would value the "database", the Government's overwhelming evidence as to the cost of the databases, and Mr. Lewis' repeated assertions to the Defense that he did not know why he was testifying and could not value information, the Defense defended this case by maintaining that PFC Manning did not steal or purloin the *databases*—not that PFC Manning did not steal or purloin information contained in the databases.

13. Now, after the close of evidence, the Court has grafted onto the Charge Sheet the word "information" – something that the Defense did not know it had to defend against until *after* it had cross-examined Government witnesses and *after* it had called its own witnesses. In short, the Defense did not know of the case to meet until 24 July 2013, almost two months into the trial, and the day before closing arguments. The Defense is now left to hope that the Government has not presented enough evidence to prove a charge that the Defense did not actually defend against and it does not believe the Government actually charged.

14. If the Defense had known that when the Government charged databases, it really meant information, the Defense would have defended this case very differently. The inability to do this, and the after-the-close-of-evidence notification that "database" apparently equals "information," has prejudiced the Defense irreparably.

15. First, the Defense would have challenged by way of motion in the summer of 2012 whether section 641 could even apply to information (when it brought all its other motions). As it stood now, the Defense had one day to provide the Court with case law on the issue. After a ruling on the issue in the summer of 2012, the Defense would have tailored its case accordingly.<sup>2</sup>

16. Further, and more importantly, if the Defense knew that "information" is what was alleged to have been stolen or purloined and that the section 641 offenses would turn in part on whether the information had a value of more than \$1000, the Defense would have requested a Government-appointed expert (much like a computer forensics expert or a security expert) so that the expert could have testified in the Defense's case-in-chief. See R.C.M. 703(d). If this

<sup>2</sup> The Defense would also have argued that one cannot have a theft of information where the Government has not lost possession of the original information. From the Court's Ruling, it appears that the Court has already made this determination based on a footnote in a Fourth Circuit case without the Defense being able to advance this argument. See Ruling p. 6.

request were denied, the Defense would have sought out an economist or other expert with knowledge about the value of information to testify and provide a countervailing opinion to Mr. Lewis.

17. The Defense would also have requested an expert on counter-intelligence to understand the specifics about the artificial market that Mr. Lewis testified about. This would have enabled the Defense to better cross-examine Mr. Lewis on his opinion on the value of the information. In addition, the Defense would have had this expert testify to the artificial nature of the "spy vs. spy" market that Mr. Lewis relied upon. Such a witness could have testified regarding how the amount paid for any item has little to do with the information within the item and more to do with establishing a relationship with the seller. Additionally, this witness could have testified that sometimes a government would purchase information for reasons other than to establish a relationship with the seller. For instance, a government may knowingly purchase information from a double agent just to see what the United States is willing to sell. This would demonstrate that the thieves' market relied upon by Mr. Lewis does not reflect an accurate assessment as to the worth of information itself.

18. Additionally, the Defense would have filed a motion to preclude Mr. Lewis from testifying and from being qualified as an expert. The Defense would have fully briefed this issue with reference to relevant case law. The Defense interviewed Mr. Lewis on numerous occasions prior to the case and Mr. Lewis repeatedly indicated that he did not know why he was testifying, he did not consider himself an expert on the value of information, and he would not be able to provide any value for documents. In fact, on the Friday prior to Mr. Lewis testifying on the Monday, he still held this position. *See* Affidavit of Mr. Cassius Hall. After apparently being coached/prepped by the Government, Mr. Lewis' opinion suddenly changed and he now felt qualified to opine as to the value of the information. Mr. Lewis' opinion lacked reliability and any of the hallmarks of expert testimony. If the Defense had known that this would now be the evidence on valuation (rather than the mountains of evidence the Government adduced regarding the cost of creating the database), the Defense certainly would not have proceeded as it did. The Defense would also have sought the underlying documentation that Mr. Lewis chose not to use to verify his valuation guess in order to see if it could truly be compared with the charged records in this case. Given the unreliability of Mr. Lewis' testimony, the Defense still submits that this Court should have granted the motion to strike his testimony. *See United States v. Horning*, 409 F.2d 424 (4<sup>th</sup> Cir. 1969).

**C. The Defense Has Been Irreparably Prejudiced By the Court's Ruling that Even Though Copies Were Apparently Stolen or Converted, the Government Can Value the Originals**

19. The Court also has apparently accepted the Government's position that there is no distinction between original records and copies of records both for identifying what was allegedly stolen and for placing a value on it. *See* Ruling, p. 7, 8. The Court, along with the Government, conflates two distinct sets of records (the original records and the digital records) in order to potentially make out a 641 offense. The Court states:

The Government is charging the accused with stealing and purloining the databases, electronic records, and information therein, at issue by accessing the relevant database, extracting the records from the database management system

structure, placing the information on private platforms or digital media while in the 2nd Brigade Sensitive Compartmented Information Facility (SCIF) at Forward Operating Base (FOB) Hammer, and asporting the downloaded records, and information contained therein, to the accused's personal platforms or digital media outside the SCIF in his housing unit.

*See* Ruling, p. 7. Here, the Court fails to distinguish between the original records ("extracting the records from the database management system") and the copies of the records ("asporting the downloaded records ... to the accused's personal platforms"). Further confusing the issue is the Court's next sentence: "The Government's theory is that the accused knowingly converted the records ... sending them to WikiLeaks." *Id.* at p. 7-8. Clearly, here there is no question that the records that PFC Manning sent to WikiLeaks were *copies* of records that he maintained on CD. However, the Court is allowing the Government to argue and introduce value of the production of originals when what the Government is saying is that PFC Manning converted the copies.

20. The Court believes that "SPKC of electronic data doesn't compare neatly to cases where the defendant made photocopies of government records, replaced the originals, and SPKC the photocopies. With SPKC, there are no copies to steal until the accused accesses the digital information and makes the extraction. The original digital database and records remain in the database management system during and after extraction." *Id.* at p. 7. The Defense sees no distinction between physical copying (in the form of photocopying or taking a picture) and digital copying. And there is no authority anywhere in the section 641 case law for allowing the cost of production of original records to be valued when what is stolen or converted are the copies. *See e.g. United States v. DiGilio*, 538 F.2d 972, 977 (3<sup>rd</sup> Cir. 1976)(court held that the "a duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen." In terms of valuing this *duplicate* copy, the court held: "Irene Klimansky availed herself of several government resources in copying DiGilio's files, namely, government time, government equipment and government supplies."); *United States v. Hubbard*, 474 F. Supp. 64 (D.C.D.C. 1979) (court allowed prosecution to proceed on theory that "the copies, allegedly made from government documents, by means of government resources, are records of the government, and thus the copies were stolen").

21. The Court draws a distinction between cases "where the defendant made photocopies of government records, replaced the originals, and SPKC the photocopies. With SPKC, there are no copies to steal until the accused accesses the digital information and makes the extraction. The original digital database and records remain in the database management system during and after extraction." *Id.* The Defense does not understand this apparent distinguishing basis. How is this any different, for instance, than seeing a classified memo on a desk and taking a picture of it (without moving it) and then sending the picture of it to someone not authorized to receive it? There is no support for treating copying of digital information any differently than copying of physical information and the Government has provided none. The Defense, based on a good-faith reading of section 641 case law, was not on notice that it would have to defend against the value of stolen originals when it is clear that what was potentially stolen were copies.

22. This is exactly the sort of mix-and-match theory of valuation that the Defense cautioned against in its Motion to Dismiss and that the Defense believes is not permitted by the section 641



case law. The Court's ruling, after the close of evidence, that the Government can introduce value of the original copies even if copies were stolen (because "electronic data doesn't compare neatly to cases [involving tangible data]") has irreparably prejudiced the Defense.

23. The Defense allowed the Government, in its Stipulations of Expected Testimony, to bring in testimony related to the cost of production of original records. Since, based on a good-faith (and the Defense submits, correct) reading of the section 641 case law, this evidence would be irrelevant where the accused stole a copy of a record, the Defense did not object to its introduction or cross-examine on it. If the Defense had known that the Court would permit the Government to allege that PFC Manning stole copies (without actually even having to amend the charge sheet), but prove the value of creating the originals, the Defense would have vigorously cross-examined all the Government's witnesses on this. The Defense would never have entered into several of the Stipulations of Expected Testimony if it were at all apparent that the Government would be allowed to value original records, rather than databases.

#### **D. The Defense Is Not At Fault For Failing to Request Further Specificity**

24. The Court appears to fault the Defense for not requesting additional specificity in the Bill of Particulars on the *res* alleged to have been stolen. See Ruling ("In the bill of particulars, the Defense posed questions with regard to the Government's theory of prosecution. The Defense did not seek more specificity as to the items charged. Nor did the Defense seek clarification after receiving the Government's response."). The Court ignores the fact that there was no need to request "further clarification" given that the Government stated that it was "clear" what property was alleged to have been stolen or converted—specific, identifiable databases (CIDNE, NCD and SOUTHCOM). The Court indicated at the time that the details provided by the Government provided sufficient notice of the charges against the accused. The Defense was not obligated to further ask the Government, "Are you sure you don't mean information? It looks like you probably meant information, so maybe you should change the charge sheet before referral."

25. This entire case proceeded on the theory that PFC Manning stole or converted the "databases"—that is why the Government adduced, and was permitted to adduce, evidence of the creation of a database. The Government's actions in seeking out witnesses and presenting a large volume of evidence related to the creation of the database makes it clear what the Government really sought to prove: that PFC Manning stole databases. It is ironic that the Defense was supposed to read into the word "database" the concept of information, all while the Government was doing its best to present every bit of available evidence valuing the actual CIDNE, NCD and SOUTHCOM databases (excluding the value of the information).

#### **E. The Defense is Still Not Clear on What PFC Manning is Alleged to Have Stolen and How that Can be Valued**

26. The Defense believes, based on the Court's Ruling, that the Government no longer has to prove that PFC Manning stole "databases" in the sense of the actual CIDNE, NCD, or SOUTHCOM databases (i.e. the receptacle for records). However, the Government has already admitted a mountain of evidence on the actual value of these databases. Apparently, even though the Government did not know it, all that evidence was entirely irrelevant to proper



valuation to what the Government should have charged (copies of records or information).<sup>3</sup> So now the Defense is supposed to read “database” as really signifying “records” or “information.”

27. The Defense submits that PFC Manning did not steal or convert original records; and to the extent that he stole or converted anything, it was a copy of those records. The Court has accepted the Government’s view, completely unsupported by authority, that there is no difference between the two. So apparently, the Government is permitted to argue that PFC Manning stole copies by giving records to WikiLeaks, but gets to value the original records. The Defense is not sure what exact method of valuation the Government will rely on and has not had an opportunity to cross-examine on this issue or request clarification at a meaningful juncture of these proceedings. The Defense submits that the cost of production of records is the time it takes for someone to enter the records onto a database. The Government has not introduced any evidence of this, so the Defense assumes that the Government will argue that the cost of harnessing and assimilating the information that eventually goes into the record is appropriate for cost of production. So, for instance, if it took 3 years to compile a detainee assessment brief, then 3 years of JAG time, commander time, etc. would establish the cost of production (such that the one detainee assessment brief might be worth \$500,000). The Defense submits that this is not a permissible valuation method for a record. But the key point is that the Defense has not had any opportunity to contest this method of valuation—because the case is already over and the Defense did not know until today that the Court would permit valuation of an original record when what was allegedly stolen was a copy or information. The Government may alternatively try arguing a “cost of production” for information. No court, to the Defense’s knowledge, has allowed such a valuation theory to proceed. The point is that at this late date, the Defense is still not clear on what valuation methods are permitted and for what property. But even if it were, there is nothing the Defense can do about this, since the parties are on the eve of closing arguments.

#### **F. The Amendments That Allege “A Portion” of the GAL or of a Database is a Major Amendment and Has Caused Unfair Prejudice**

28. The Court believes that changing Specification 16 of Charge II to read that PFC Manning stole or converted “a portion” of the GAL is not a major amendment. The Defense disagrees and believes that this is a major amendment that seriously prejudices the accused and warrants relief under R.C.M. 915.

29. The Defense did not focus its questioning on establishing whether the military addresses found on PFC Manning’s computer constituted a subset of the USF-I GAL; it focused its questioning on whether the addresses constituted the USF-I GAL. If the Defense had known that the charge would shift from being “the USF-I GAL” to “a portion of the USF-I GAL,” the Defense would have questioned Government witnesses on whether the email addresses found on his computer comprised a “a portion” of the USF-I GAL and the basis for that opinion. The Defense would not have simply let what would appear to be irrelevant statements go unchecked if it now knew it was now defending against PFC Manning stealing “a portion” of the USF-I

---

<sup>3</sup> The fact that the Government itself was incredibly confused on what it was valuing (the database, to include it supporting infrastructure) suggests that the Defense’s belief as to the identity of the allegedly stolen property was entirely reasonable.

GAL (e.g. it would have cross-examined Chief Nixon further on his statements regarding his opinion that this might be the Division GAL).

30. Further, the Defense would also have focused its questions regarding valuation on the value of a subset of the USF-I GAL, not on the value of the USF-I GAL as a whole. The Defense would have also objected to the Government eliciting testimony about the value of the USF-I GAL as a whole if the Government was merely proving that PFC Manning took "a portion" of the USF-I GAL.

31. Similarly, the amendment that PFC Manning stole a "portion" of a database is a major amendment because it impeded the ability of the Defense to cross-examine on the value of a "portion" of the database. The Defense would have interviewed witnesses and ascertained for itself what the cost of production of these records would be. The Defense would not be left simply hoping that the Government has not met its burden of proof.

#### CONCLUSION

32. It is clear from federal case law that "records" and "information" are different things. The Court's conflating of "database" and "records" and "information," after the close of evidence, is not a fair or accurate reading of the law and unfairly prejudices the accused in this case.

33. The Government has pushed this case beyond the bounds of legal propriety. If the Government meant "information", it should have charged information. We should not have to rely on Black's Law Dictionary to get us there. If the Defense knew that the property allegedly stolen was "information" it would have proceeded in an entirely different fashion. This is true as well if the Defense knew that the Court would allow the Government to value original records when no original records were stolen or converted.

34. Because all of these critical "clarifications" are coming after eight weeks of testimony, and because these offenses carry with them 50 years of potential imprisonment, and because the Defense was actually misled by the Charge Sheet, the Defense requests that this Court declare a mistrial as to the section 641 offenses. The accused is still facing the prospect of life in prison (due to what the Defense submits is an unprecedented Article 104 charge). There is no need to mar the appellate record in such a way that it clear that a substantial doubt is cast upon the fairness of these proceedings.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

I am a detailed Security Expert for the defense in the case of US v. PFC Bradley Manning. I understood that I, or my fellow expert Charles Ganiel, was required to be present at any witness interviews in which classified information would be discussed. In discharging those duties, I recall being present for at least five witness interviews with Mr. Danny Lewis.

I cannot recall the exact date of the first meeting, but I believe that it was in either late 2012 or early 2013. The meeting took place in the office Mr. Lewis occupied at the time in Quantico, Virginia. The following people were present at that meeting: Mr. Lewis, MAJ Thomas Hurley, someone from DIA, and myself. After introductions, I can recall Mr. Lewis saying that he has oversight generally into what information the enemy is looking for given his access to the ongoing counterintelligence operations. Mr. Lewis indicated that there was no way to determine the actual value of classified documents. Mr. Lewis indicated that he was not an expert in determining value of classified information. Mr. Lewis could only use the past or existing missions as a guide to make any decisions. Mr. Lewis also indicated that he was unclear what he was going to be testifying about at this trial.

The second meeting with Mr. Lewis occurred in May of 2013. That interview occurred in a conference room at my workplace at INSCOM. The following people were present at that meeting: Mr. Lewis, MAJ Hurley, and myself. From this interview, I recall Mr. Lewis indicating that there was no way of actually determining the value of classified documents. Mr. Lewis then indicated to MAJ Hurley and myself that the only things he could talk about would be what US government information adversaries would be interested in and what they would do with it. By that time, Mr. Lewis did understand what he was going to testify about, but only in general and vague terms. Mr. Lewis did not know of any training or educational classes that could train you to value classified information. Mr. Lewis asked me if I had ever heard of anything like that, and I told him I had not. Mr. Lewis told us that all we could use was historical information from similar incidents that occurred in the past. Mr. Lewis told us again that he did not consider himself an expert at valuing classified information. Mr. Lewis told us then that he had not reviewed any of the evidence in this case. Mr. Lewis also indicated that he could not remember anything specifically about the historical data that had been captured.

The third meeting occurred in June of 2013 in the days leading up to the testimony of Mr. Lewis. I recall this meeting taking place the Thursday prior to the testimony of Mr. Lewis in the defense trailer near the courtroom here on Fort Meade. The following people were present at that meeting: Mr. Lewis, MAJ Hurley, and myself. I recall Mr. Lewis saying that he was going to testify about the contents of the charged documents in this case. He also indicated that he did not then consider himself an expert at valuing classified information and that he had never considered himself an expert at it. This was the first time Mr. Lewis showed us the documents that he had pulled from his colleagues at DIA. He also indicated that he did not know how he was going to testify about the value of classified documents when he only had the contents of those documents to use in making any determination.

The fourth meeting occurred in June of 2013 in the days leading up to the testimony of Mr. Lewis. I recall this meeting taking place on a Friday in the witness trailer at the courtroom on Fort Meade. The following people were present at that meeting: Mr. Lewis, MAJ Hurley, and myself. Mr. Lewis was asked again about the nature of his testimony, and Mr. Lewis talked about the data he pulled from his

colleagues at DIA. In this meeting, Mr. Lewis again indicated that he was not an expert. I recall MAJ Hurley asking him how he could make any valuation determination, and he could only reference the documents pulled from DIA. Mr. Lewis indicated that he was not part of any valuing determinations in his official duties. Finally, he talked about failed operations and how they were or were not used in determining the value of classified documents.

The fifth meeting occurred in June of 2013 in the days leading up to the testimony of Mr. Lewis. I recall this meeting taking place on a Monday. The following people were present at that meeting: Mr. Lewis, MAJ Hurley, and myself. MAJ Hurley asked Mr. Lewis again about the value of documents. Mr. Lewis talked about the documents he pulled from DIA and how they were compiled for his testimony. Mr. Lewis also talked about his then discontinued access to the information from DIA because his role with that organization had changed.

I have talked to Mr. Ganiel. He indicated to me that he was never present for any other witness interviews with Mr. Lewis.



CASSIUS N. HALL  
Detailed Security Expert

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Accounting of Expert  
Witnesses for  
Presentencing

25 July 2013

This filing supplements Appellate Exhibit (AE) 543, the Government's Accounting of Discovery and Expert Witnesses dated 15 May 2013, wherein the United States notified the defense and the Court which witnesses it may qualify as experts, and in what field, during the merits and/or presentencing phase of trial. The United States still may qualify those witnesses who will testify during the presentencing phase of trial as experts in their respective fields. In addition, the United States may qualify the following witnesses as experts in the below fields:

a. RADM Kevin M. Donegan. The United States may qualify this witness as an expert in United States Central Command (USCENTCOM) operations from 2010 to 2012;

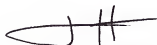
b. Mr. John Kirchhofer. The United States may qualify this witness as an expert in strategic planning for Department of Defense counterintelligence (CI) and human intelligence (HUMINT), to include strategy, policy development, and functional management;

c. MajGen Frank McKenzie. The United States may qualify this witness as an expert in USCENTCOM strategic planning from 2010 to 2012; and

d. Mr. Adam Pearson. The United States may qualify this witness as an expert in terrorist activities on the Internet.

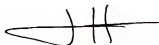
Since 15 March 2013, the defense has been on notice of the subject matter of the expected testimony for the above four witnesses. See AE 505. Based on the scope of their expected testimony, the United States has disclosed, or made available to the defense for inspection, those specific facts or data that could reasonably be identified as underlying the opinions of the above witnesses IAW MRE 705. Should the United States learn of additional specific facts or data underlying their opinions during the course of trial preparation, the United States will disclose that material and account for any such disclosure.

The above list does not account for any witnesses the United States may qualify as experts in rebuttal.



J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail on 25 July 2013.

A handwritten signature in black ink, consisting of a stylized 'J' followed by 'H' and a horizontal line.

J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

**Schedule of Government Witnesses  
for Presentencing Phase**

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

**25 July 2013**

The United States submits the below order for the twenty presentencing witnesses the United States intends to call in the above-captioned court-martial, along with the dates of their testimony. Witnesses #1-15 have coordinated their schedules to be available on the below dates and at the specified time. Witnesses #16-20 will be on-site, starting 5 August 2013, and will be standing-by, ready to testify, when time permits. Witnesses identified with a caret ("^") are witnesses the United States intends to qualify as expert witnesses. Witnesses identified with an asterisk ("\*") are witnesses for which the United States intends to elicit classified testimony in a closed session for a portion of their testimony.

**Wednesday, 31 July 2013**

1. AM - BG (R) Robert Carr^
2. PM - Mr. John Kirchhofer^\*

**Thursday, 1 August 2013**

3. AM - PDAS Elizabeth Dibble^\*
4. PM - PDAS John Feeley^\*

**Friday, 2 August 2013**

5. AM - Ms. Susan Swart^
6. PM - AMB Michael Kozak^

**Monday, 5 August 2013**

7. AM/PM - AMB Patrick F. Kennedy^

**Tuesday, 6 August 2013**

8. AM - MG Michael Nagata^\*
9. PM - Col Julian Chesnutt^\*

**Wednesday, 7 August 2013**

10. AM - Mr. James McCarl^\*
11. PM - Mr. Adam Pearson^

**Thursday, 8 August 2013**


12. AM - Mr. Randall MacRobbie^\*
13. PM - CDR Youssef Aboul-Enein^\*

**Friday, 9 August 2013**

14. AM - RADM Kevin Donegan^\*
15. PM - MajGen Kenneth McKenzie^\*

**Witnesses Standing-By**

16. COL David Miller
17. Ms. Jihleah Showman
18. CPT Steven Lim
19. SA David Shaver
20. SA Mark Mander

  
J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 25 July 2013.

A handwritten signature in black ink, appearing to read 'J. HUNTER WHYTE', with a horizontal line extending to the right.

J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel



Appellate Exhibit 617

4 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

- (1:58:31 PM) bradass87: if you had unprecedented access to classified networks 14 hours a day 7 days a week for 8+ months, what would you do?
- (12:15:11 PM) bradass87: hypothetical question: If you had free reign over classified networks for long periods of time... say, 8-9 months... and you saw incredible things, awful things... things that belonged in the public domain, and not on some server stored in a dark room in Washington DC... what would you do?

(12:33:05 PM) bradass87: in other words... he made a huge mess: "I  
(12:38:17 PM) bradass87: am sorry... im just emotionally fractured  
(12:38:12 PM) bradass87: im a total mess  
(12:41:54 PM) bradass87: I think im in more potential heat than you ever  
was  
(12:41:54 PM) info@adrianlamo.com <AUTO-REPLY>: I have more  
messages than resources available to action them. Please be very patient.  
(12:45:50 PM) info@adrianlamo.com: not mandatory  
(12:46:00 PM) info@adrianlamo.com: there are always outs  
(12:46:17 PM) info@adrianlamo.com: how long have you helped  
Wilemies?  
(12:49:09 PM) bradass87: since they released the 9/11 "paper messages"  
(12:49:38 PM) bradass87: immediately recognized that they were from an  
NSA database, and I felt comfortable enough to come forward  
(12:50:20 PM) bradass87: so... right after Thanksgiving timeframe of 2000  
(12:51:33 PM) bradass87: Hilary Clinton, and several thousand diplomats  
around the world are going to have a heart attack when they wake up one  
morning, and find an entire repository of classified foreign policy is available  
in searchable format to the public... <1  
(12:53:41 PM) bradass87: <Hilary/Hillary  
(12:54:47 PM) info@adrianlamo.com: What sort of content?  
(12:56:36 PM) info@adrianlamo.com: info @gizmodo  
(12:56:43 PM) info@adrianlamo.com: keep typing <3

(12:58:41 PM) bradass87: uhm... crazy, almost criminal political backlashes  
the top 50 versions of world events and crises... when... all kinds of stuff has  
everything from the buildup to the Iraq War during Power, to what the actual  
content of "aid packages" is: for instance, PR that the US is sending aid to Pakistan  
includes funding for water/food/clothing... that much is true, it includes that, but the  
other 85% of it is for > 16 fighters and munitions to aid in the Afghanistan effort, so  
the US can call in Pakistanis to do aerial bombing instead of Americans potentially  
killing civilians and causing a PR crisis  
(1:00:39 PM) bradass87: there's so much... it affects everybody on  
earth... everywhere there's a US post... there's a diplomat, scientist that will be  
targeted... instead, the Vatican, Spain, Brazil, Madagascar, if its a country, and its  
recognized by the US as a country, its got shit on it  
(1:01:02 PM) bradass87: I need one myself  
(1:01:03 PM) bradass87: its open database... world-wide anarchy in CSV  
format... its compatible with a SQL database... its browser-based... its beautiful  
and beautiful  
(1:01:30 PM) info@adrianlamo.com <AUTO-REPLY>: I have more messages  
than resources available to action them. Please be very patient.  
(1:11:54 PM) bradass87: and... its important that it gets out... I feel, for some  
bizarre reason  
(1:12:02 PM) bradass87: it might actually change something  
(1:13:10 PM) bradass87: just... dont wish to be a part of it... at least not now.  
im not ready... i wantn't need going to prison for the rest of my life, or being  
executed so much, if it wasn't for the possibility of having pictures of me... plastered  
all over the world press... its boy  
(1:14:11 PM) bradass87: I've totally lost my mind... i make no sense. the CPU is  
not made for this motherfucker!  
(1:14:42 PM) bradass87: uhm boy/ies a boy

(02:50:44 PM) bradassa7: [17] SIPDIS--  
 "formessagesinintendedforautomaticWebpublishingtothe originating  
 post's or office's Web site. (see 5 FAM 770 for policies regarding  
 information on Federal Web site and 5 FAM-2 H-443.1, When and  
 How to Use SIPDIS);  
 (02:51:58 PM) bradassa7: <http://www.state.gov/documents/organization/89284.pdf>  
 (02:52:03 PM) bradassa7: [reference]  
 (02:52:47 PM) bradassa7: state dept fucked itself... placed  
 volumes and volumes of information in a single spot, with no security  
 (02:53:28 PM) info@adrianfamo.com: only the people you trust  
 can fuck you - infowise ;>  
 (02:54:03 PM) bradassa7: so anything published, and classified  
 up to SECRET//NOFORN

#### TIMELINE

Abroad Links  
 1) Iraq NOAC T's (Took 8 Jan 10. Given from NOC Card to WL on 1 Feb 10. WL publishes 22 Oct 10)  
 2) Afghanistan SIGACTS (Took 8 Jan 10. Given from SIG Card to WL on 3 Feb 10. WL publishes 23 Feb 10)  
 3) Bahrain al-13 Cable (Took 1 Feb 10. Given to WL on 19 Feb 10. WL publishes 28 Feb 10)  
 4) Iraq Value (Took 1 Feb 10. Given to WL on 23 Feb 10. WL publishes 28 Feb 10)  
 5) AICTE Report (Took 1 Mar 10. Given to WL on 8 Mar 10. WL publishes 28 Feb 10)  
 6) CTMD Documents (Took 7 Mar 10. Given to WL on 8 Mar 10. WL publishes 28 Feb 10)  
 7) OIA Documents (Took 22 Mar 10. Given to WL on 23 Mar 10. WL publishes 28 Feb 10 and 28 Aug 10)  
 8) Afghanistan Cable (Took 18 Apr 10. Given to WL on 18 Apr 10. WL starts to publish 28 Nov 10 and publishes all ~~unclassified~~ cables on 2 Sep 11)  
 9) French Value and French Intelligence Reports (Took on 17 Apr 10 video. Took on 18 Apr 10 11-4 for responses. Given to WL on Apr 19. WL starts to publish 10)  
 10) Outlook Smartphone Package Server Global Addresses (provided 11 May. Never Given to WL)

## The Truth

## Defense Exhibit R

### Testimony of Ms. McNamara

- "I can apply what I learn to provide more information to my officers and commanders, and hopefully save lives..."
- "I'm more concerned about making sure that everyone, soldiers, marines, contractors, even the local nationals, get home to their families."

### Defense Exhibit R

- "I feel a great responsibility and duty to people ... it's strange, I know."
- "I place value on people first."

### Defense Exhibit R

- "I've got foreign affairs on my mind constantly now ... One of the bad parts of the job, having to think about bad stuff."
- "Sometimes I wish it were all black and white like the media and politicians present it ... him, he's a the bad guy, oh and he, he's the good guy... it's all shades of blurry grey."

### Adrian Lamo

- Believed PFC Manning was:
  - Young
  - Idealistic
  - Well-intentioned

### Adrian Lamo/PE 30

Testified that PFC Manning believed:

- Information would have an impact on the entire world
- Information would disclose casualty figures in Iraq
- Diplomatic cables explained how we exploited others

### Adrian Lamo/PE 30

Testified that PFC Manning believed:

- It was important that the information got out
- He could not separate himself from others
- He was connected to everybody
- We were all distant family

### Adrian Lamo/PE 30

Testified that PFC Manning told him:

- That he cared about others
- That he wanted to make sure that everyone was okay
- That he separated himself from other analysts because he did care about people

### Adrian Lamo/PE 30

Testified that PFC Manning told him:

- He followed humanist values
- He wore custom ID tags that said "Humanist"
- He was troubled that no one seemed to care

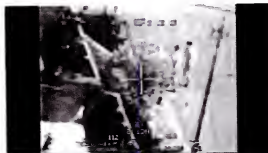
### Adrian Lamo/PE 30

Testified that PFC Manning told him:

- He was hoping to spark worldwide discussion, debates, and reforms
- He wanted people to see the truth
- He was hoping people would change based upon having the information

### Significant Events

- Christmas Eve EFP SIGACT: Defense Exhibit E – CW2 Ehresman
- Arrest of 15 Iraqis for printing literature critical of Iraqi government: PE 123 and SGT Sadtler
- Apache Video: PE 30
- Farah Video: PE 30
- Day to Day Activities



### Government Version

### Government Version

- PFC Manning Deploys in November of 2009
- Within two weeks, PFC Manning is working for Wikileaks
- MOTIVE?

### Government's Proof

- 2009 Wikileaks Most Wanted List
- Jason Katz's Computer
- Adrian Lamo Chat
- USF-I GAL
- Wiping Computer
- Showman's allegations

### 2009 MW List

- Tried to make it seem like a evil list by giving the sort version only
- List of events that reporters, humanitarians, activists, and NGOs want to know
- Could only remotely tie PFC Manning to 4 of the 78 things for U.S. and the same 4 for the several hundred on the list

### Jason Katz's Computer

- No tie between PFC Manning and Jason Katz
- Jason Katz has Farah video on computer 15 December 2009
- Forensics from 1 December 2009 forward show PFC Manning never accessed the CENTCOM Farah video

### Jason Katz's Computer

- To give to Jason Katz and WL, PFC Manning must have taken the Farah video in November
- Centaur Logs - Net Flow
- Intellink Logs - 30 November search for "CENTCOM"

### Jason Katz's Computer

- Encrypted Farah video that WL did not ask for in 2009 MW List
- Waited five months to send the supporting Farah documentation: 15-6 and PPT slides that were at the same location
- Pulled all of that information but the encrypted Farah video in April of 2010

### Jason Katz' Computer

- SA Shaver - evidence PFC Manning pulled a video from the T-Drive in a folder labeled Farah (TGT1.wmv)
- Government never disputed that an unencrypted Farah video was available on the T-Drive



### WL 8 Jan 2010 Tweet

- Tweet that WL had an encrypted video that they needed super computer assistance on.
- How did WL get the encrypted video?

**JASON KATZ**

### Jason Katz

- Source of video for Wikileaks
  - Mr. Katz was using a program that allowed him to transfer files between his computer and to another computer not his home computer - Mr. Withers
  - Mr. Katz had a password cracking software on his computer - Mr. Withers
  - Mr. Katz had access to BNL's super computer system - Mr. Fung

### Adrian Lamo Chat/PE 30

### Adrian Lamo Chat/PE 30

- Gov claims PFC admitted to giving the encrypted video
- T-Drive (TGT1.wmv) on two locations

### Farah Video

- PFC Manning was the most organized analyst he had ever seen in his 20 years – CW4 Hack
- He had "several directories and subdirectories" his files were "very neatly organized" – CW4 Hack
- Shaver – video pulled from a folder labeled "Farah" and placed on PFC Manning's computer at two locations labeled "Farah"

### Farah Video

- Why does the Government reject the idea that PFC Manning gave the Farah video along with the other Farah documents in April 2010?

It doesn't fit its fictional story

### USF-I GAL

- WL Tweet requested .mil addresses not Iraq e-mail addresses
- Forensics for everything – but no forensics for sending the Division GAL to anyone
- Common sense explanation for why PFC Manning would want to see if he could download the Division GAL

### The USF-I GAL

- Why does the Government want to argue PFC Manning "stole, purloined, or knowingly converted" the USF-I GAL?

It fits its fictional story

### Wiping Computer

- If you were covering your tracks, wouldn't you wipe your computer in February? (Cable; Apache video)
- March? (ACIC; DABs; OGA)
- April? (NCD; Farah Video and Files)
- May? (No longer in T-SCIF)

### Wiping Computer

- 7 Pass Wiping – is minimum amount to wipe computer – Mr. Johnson
- Wiping a computer due to being in an environment like Iraq
  - DCGS-A computers needed to be wiped on a frequent basis
  - Reinstalling operating system and clearing unallocated space is normal

### Wiping Computer

- Why is the Government trying to make a big deal out of PFC Manning's decision to reinstall his operating system on 25 January 2010 and clear his unallocated space on 31 January 2010?

It fits its fictional story

### Showman's Allegations

- Ms. Showman
  - Never reduced to written counseling
  - Did not mention when first interviewed by CID after arrest
  - Incredible story regarding reporting to then MSG Adkins (possible spy)
  - Motive to fabricate (punch; EO complaint; statements in movie; Twitter account)

### Showman's Allegations

- Mr. Adkins
  - Does not remember/recall Ms. Showman telling him anything
  - Never wrote about alleged statements in his MFRs
  - Did not mention in any of his interviews by CID or for 15-6
  - In GOMAR Rebuttal stated PFC Manning never made disloyal comments
  - Admin Reduction Board Statement

### Arrogance v. Anonymity

- Seeking Fame?
  - "He wanted to guarantee his fame."
  - "He wanted attention from the press."
  - "He sought publicity."
  - "Collected trophies."
- Wanted Anonymity?
  - "Obsessed with covering his tracks."
  - "Wanted them to protect the source."
  - "He tried to erase any evidence of what he did."

### Good Soldier/Hacker

- Is he the "go to analyst" or not?
- Spending time "systematically harvesting" information or is he getting his work done on time?
- Constantly searching for WL or is he the most organized analyst in the S2 Section?

### Worst Employee of All Time

- At MOST, only searched for 4 of the 78 items on 2009 MW List (his so-called "guiding light").
- Unlimited access and unlimited ability to download and save but only sends limited items

### Government Version

- Story does not make sense
- Story is not consistent with the facts or even internally consistent
- MOTIVE – What case did the Government participate in?

### Charges

### Charges

- PFC Manning was young and naive, but he wasn't wrong
- Look at the evidence and compare with the statements
- No one wants to question the OCA
  - TTPs, troop movements, close air support, weapons systems, unit identifiers, DUSTWUN procedures

### Apache Video

- Specification 2 of Charge II
  - Not closely held or classified
  - Quoted verbatim in Finkel's "The Good Soldiers"
  - CENTCOM FOIA Response
  - PE 15 - CD in CHU labeled Reuters FOIA Request
  - Edited for Reuters (copy for Reuters)
  - Could NOT cause damage only embarrassment - DE O

### Farah Video

- Specification 11 of Charge II
  - No connection between Manning and Mr. Katz
  - Mr. Katz's video matched CENTCOM
  - Mr. Katz is the source
  - No forensics before April 2010 dealing with Farah
  - Fantastical version offered by the Government
  - Shaver's common sense version

### Farah Documents

- Specification 10 of Charge II
  - Documented a large-scale civilian casualties (CIVCAS) incident that received worldwide attention - LCDR Hoskins
  - Did not consider open source material, unclassified publications (ARs and FMs) - LCDR Hoskins
  - Look at the basis provided by the Government's witnesses - Mr. Travieso

### 1030 and Article 92

- Specification 13 of Charge II and Specifications 2 and 3 of Charge III
  - Wget was not prevented from running and soldiers allowed to add executable files to computer
  - Even if it was unauthorized software does not equal an access restriction
  - No such thing as an implicit access restriction
  - No AUP

### 1030 and Article 92

- No Rules: The Unit
  - No restrictions on downloading - COL Miller
  - No restrictions on downloading from NCD
    - CPT Lim
  - No training on any so-called download restrictions and PFC Manning did not need to hack or circumvent anything to gain access to NCD - CPT Cherepko
  - No restriction on using an executable files from CD or desktop or to download from SIPRNET - CW2 Ehresman

### 1030 and Article 92

- No Rules: NCD – Mr. Wisecarver
  - No restrictions on manner of downloading
  - No restrictions on access other than access to SIPRNet
  - DOS relied upon receiving agencies for any restrictions
  - Purpose was to share cables
  - Multiple screens can be opened for printing and saving

### 1030 and Article 92

- SA Shaver
  - Wget did not provide greater access
  - Wget simply automated the click-open-save process
  - Wget accessed each cable individually
  - Wget is not a nefarious program – it is just a simple command line program

### 1030 and Article 92

- No T-SCIF SOP – CPT Lim
  - Unclear what was as was not permitted in T-SCIF ("knowingly") – CPT Keay
    - COL Miller/SPC Showman – Movies and Music good
    - CPT Lim – Movies bad, Music good
    - CPT Cherepko – Movies and Music bad
    - CW2 Balonek – Did not know if Movies and Music were bad or not
    - SGT Madaras – Movies and Music were allowed
    - Mr. Milliman – NO Music, Movies or Games

### 1030 and Article 92

- AR 25-2
  - Book Answer/Real World Answer – Mr. Weaver
  - Things were different when deployed as opposed to in garrison – CW2 Balonek
- mIRC Chat
  - Not authorized as baseline – Mr. Kitz
  - CDR must request – Mr. Kitz
  - Authorized on DCGS-A – Mr. Milliman

## 1030 and Article 92

- Executable Files and Games
  - CPT Chrepeko - Executable files are same as games - not allowed. No authorized T-Drive folder for music, movies, games, executables
  - CW2 Ehresman - Executable Files and Games allowed
  - SPC Showman - Games allowed and PFC Manning placed mIRC Chat on her computer
  - SGT Madaras - PFC Manning worked on computers, placed mIRC Chat on his computer, silence on the Issue of what was and was not allowed
  - CPT Fulton - mIRC Chat placed as an executable file on her computer

## Article 92

- Specification 1 of Charge III (not to cover tracks)
- No T-SCIF SOP - CPT Lim
  - Breaking Passwords - Mr. Milliman
  - Asked to Break Passwords - SPC Showman
- AR 25-2
  - Book Answer/Real World Answer - Mr. Weaver

## 641 Offenses

- Specifications 4, 6, 8, 12, and 16 of Charge II and Specification 4 of Charge III
  - Government failed to prove BRD PFC Manning stole, purloined, or converted the charged databases
  - Government failed to prove PFC Manning used an information system in violation of AR 25-2

## 641 Offenses

- Value of Original Records
  - CIDNE I and A - no evidence of value from Mr. Bora
  - DAB - no evidence of value from Mr. Motes (27-10 example)
  - NCD - no evidence of value from Mr. Wisecarver
  - GAL - no evidence of value (27-10 example)



### 641 Offenses

- Value of Copy
  - CIDNE I and A - no evidence of value
  - DAB - no evidence of value
  - NCD - no evidence of value
  - GAL - no evidence of value

### 641 Offenses

- Value of Information
  - CIDNE I and A - Mr. Lewis' Guess
  - DAB - Mr. Lewis' Guess
  - NCD - Mr. Lewis' Guess
  - GAL - Mr. Lewis' Guess

### 641 Offenses

- Mr. Lewis
  - Didn't initially know why he was testifying
  - Month before testifying said he could not put value on classified information
  - Days before testifying did not consider himself to be a valuation expert
  - Never valued information before during his entire career
  - Never even tried to verify his guess
  - Not a thieves market: artificial market

### USFI-GAL

- Wrongful
  - Chief Nixon - No rules against downloading .mil addresses
  - SA Williamson - the DoD warning banner did not prohibit the downloading
  - AKO Accessed at home
- Steal or Convert
  - No evidence that PFC Manning did anything with email addresses
  - Where is evidence of spearfishing?

### USFI-GAL

- Value
  - Failed to offer any evidence as to actual value of email addresses that are temporary
  - Chief Rouillard said 10 to 15 minutes from receiving the form - filling it out - and then populating into GAL
  - Purely speculative information offered by Mr. Lewis

### DABs

- Specification 9 of Charge II
  - Baseball Cards - Col. Davis
  - GTFR - limited purpose
  - CSRTs and ARBs
  - Habeas Litigation
  - Look at highlights - Col. Davis
  - 4 of the 5 charged DABs deal with individuals that have been released
  - Look at portion that is not highlighted and ask could this be used for prohibited purposes?

### CIDNE-I AND CIDNE-A

- Specifications 5 and 7 of Charge II
- Historical document
  - Records past events - the 5 Ws
  - Events observable by enemy
  - PFC Manning understood use of SIGACTs
- Government Continued to Use
  - Analysis is what is important - Mr. Hall
  - Look at basis for so-called harm
  - NO CALL Update

### ACIC Document

- Specification 15 of Charge II
  - Collection of open source information
  - Wasn't a request document - Ms. Glenn
  - Assumptions and presumptions, but no sources - Ms. Glenn
  - Professor Benkler - poorly written piece that was based upon open source without any supporting documentation for conclusions

### Documents

- Specification 3 of Charge II
  - Read what was discussed
  - Read the purpose of the discussions
  - Compare against Stipulations of Expected Testimony
  - Ask if this really is the type of information that could be used for prohibited purposes

### Specification 1 of Charge II

- Caused to be Published
  - Gave documents to Wikileaks, but did not control if Wikileaks would publish them
  - Arrest of 15 individuals printing anti-Iraq government literature - PE 123
  - Wikileaks and other media partners (New York Times, Guardian, Der Spiegel) decided what to publish and how much to publish, if anything

### Specification 1 of Charge II

- Wanton
  - Selected a legitimate journalistic organization
  - Had access to everything on SIPRNet
  - Selected only those items that he believed could not cause damage

### Specification 1 of Charge II

- Wanton
  - Evidence of path of the intelligence from PFC Manning to the enemy is circumstantial evidence to disprove wanton
    - UBL Stipulation of Fact
    - Adam Gadahn (had to tell AQ and AQAP to go to Wikileaks) - PE 182

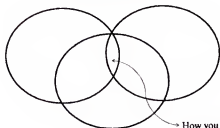
### Article 104

- Actual Knowledge
  - Government failed to offer any evidence as to actual knowledge
  - Government failed to offer any evidence as to "general evil intent"
  - Government offered only evidence of "Inadvertent, accidental, or negligent" disclosure to enemy

### Article 104

- Circumstantial Evidence
  - Training of intelligence analyst
  - PowerPoint Presentation during AIT
  - Accessible to the enemy on the internet (analyst vs. truck driver)
  - ACIC Document

### Article 104



### ACIC (Page 6)

(17) WikiLeaks.org supports the US Supreme Court ruling regarding the unauthorized release of the Pentagon Papers by Daniel Ellsberg, which stated that "only a free and unrestrained press can effectively expose deception in government." The WikiLeaks.org Web site further states the following:

"We aim for maximum political impact. We believe that transparency in government activities leads to reduced corruption, better governments, and stronger democracies. All governments can benefit from increased scrutiny by the world community, as well as their own people. We believe this scrutiny requires information. Historically that information has been costly—in terms of human life and human rights. But with technological advances—the Internet, and cryptography—the risks of conveying important information can be lowered." [10]

## ACIC (Page 7)

April 2007 Wikileaks.org staff members and various authors and contributors have written numerous news articles and posted the raw data in spreadsheets or Structured Query Language (SQL) data base so anyone can examine the information, conduct research, comment upon, discuss the various units, see the items of equipment, see what they do, and draw their own conclusions about the strategic, political, military, and human rights significance of the information [15]

## ACIC (Page 9)

**Warning:** The foreign staff writer for Wikileaks.org, Julian Assange, wrote several news articles coordinated other articles, and developed an interactive data base for the leaked documents. In addition, other Wikileaks.org writers and various writers for other media publications wrote separate news articles based on the leaked information posted to the Web site. Assange and his coauthors claim that the 2,000 pages of leaked US military information provides unit names, organizational structure, and tables of equipment (TOEs) for the US Army in Iraq and Afghanistan. They also claimed that unidentified persons within the US government leaked the information to facilitate action by the US Congress to force the withdrawal of US troops by cutting off funding for the war [16]

(U//FOUO) Assange and other Wikileaks.org writers purport that the leaked sensitive TOE information reveals the following

## ACIC (Page 10)

(U) One Wikileaks.org news article also documents the use of IEDs by foreign terrorists and insurgent groups and claims that the IED threat has resulted in a shift in DoD funding priorities, similar to the Manhattan Project to develop atomic weapons in World War II, for current research, development and fielding of IED countermeasures through the Joint IED Defeat Organization. In addition, the author of the article attempts to provide a cost-to-benefit analysis of these IED tactics and countermeasures. The author claims that the leaked information reveals that 12,097 Warlock, Counter IED (Remote-controlled Improved Explosive Device) Electronic Warfare (CREW), systems are in Iraq and that the purpose of the Warlock is to jam radio signals from devices such as mobile phones to prevent such signals from detonating IEDs

## ACIC (Page 12)

(U//FOUO) Julian Assange also stated in his news articles involving the TOE information that persons were welcome to assist in the following future actions and areas of research involving the equipment listings

## ACIC (Page 14)

(U//FOUO) Another example of leaked information posted to the WikiLeaks.org Web site on or about 7 November 2007 is an outdated copy of the Joint Task Force-Guantanamo, Camp Delta Standard Operating Procedures (SOP) marked as UNCLASSIFIED//FOUO, signed by MG Miller and dated 28 March 2003. A news article written by WikiLeaks.org staff writers, also posted on 7 November 2007, claims the SOP reports systematic methods for preventing illegal combatants and detained prisoners incarcerated at Joint Task Force-Guantanamo facilities at Camp Delta from sundering with the International Red Cross, as well as the use of extreme psychological stress as a means of torture against detainees. The unauthorized release of the SOP has prompted authors posting to the WikiLeaks.org Web site to claim that the document proves the US Army was torturing and violating the human rights of detainees held at Guantanamo Bay. This SOP was also the subject of a lawsuit by international human rights groups and a domestic civil rights organization requesting the release of the document under the US Freedom of Information Act [13].

## ACIC (Page 15)

objectives. WikiLeaks.org claims the document was leaked by a source it refers to as "Peyton" who is described as a former employee of NGIC. Both a copy of the actual NGIC classified report (in PDF) and the WikiLeaks.org news article were posted on the WikiLeaks.org Web site. A variety of newspapers, wire services, and other news and media organizations wrote numerous articles based on the original WikiLeaks.org news article and actual classified document posted to their Web site [15].

WikiLeaks.org and some other news organizations did attempt to contact the NGIC personnel by e-mail or telephone to verify the information. Such efforts by WikiLeaks.org to verify the information are in contravention to its stated policy not to attempt to verify the information it receives from its sources. WikiLeaks.org went forward with publishing their news article based on the classified NGIC report although they did not receive a response to their inquiry. This is of interest because some journalists exploit the lack of a response to their inquiries by implying that a refusal to respond, failure to respond to a FOIA request, or failure to verify or receive other information presumes that those failing to respond have something to hide. This further weakens

## ACIC (Page 16)

possibilities. A former NGIC employee would be regarded by many as a highly credible source and either taken at his or her word or asked to provide other bona fides to verify the employment claim. Given the high visibility and publicity associated with publishing this classified report by WikiLeaks.org, however, attempts to verify the information were prudent and show journalistic responsibility to the news/orthodoxy or fair use of the classified document if they are investigated or challenged in court [16].

## ACIC - Professor Benkler

- ACIC – poorly written and researched
- Wikileaks does verify its information before publication
- Wikileaks received numerous awards for its journalistic endeavors
  - 2008 Index on Censorship Award
  - 2009 Amnesty International New Media Award
- MAJ Fein's Characterization of the quality of Professor Benkler's work

### Article 104

- Actual Knowledge
  - ACIC document: Government does not even know if enemy went to Wikileaks
  - Intelligence GAP - Is something that we do not know (all unit witnesses)
  - Assumption - Is something we don't know (all unit witnesses)
  - No training on particular websites the enemy may have gone to
  - "Presumed" equals negligence and not actual knowledge

### Article 104

- Actual Knowledge
  - All the of forensics prove that PFC Manning never discussed the enemy or wanting to get information to the enemy
  - All of the forensics prove that PFC Manning had a good motive and not a "general evil intent"

### Article 104

- Circumstantial Evidence
  - Evidence of path of the Intelligence to enemy to disprove actual knowledge
    - UBL Stipulation of Fact
    - Adam Gadahn - PE 182
  - Junior analyst still learning how to connect all the dots (SFC Anica; CPT Fulton; CW2 Balonek; CW4 Hack CPT Lim)
  - Limited SIPR access in Garrison (SFC Anica and CPT Lim)

The Truth

Appellate Exhibit 619  
have been entered into  
the record as CD/DVDs  
and will be maintained  
with the original  
Record of Trial



Appellate Exhibit 620  
ordered sealed for Reason 4  
and Reason 8  
Military Judge's Seal Order  
dated 20 August 2013  
stored in the original Record  
of Trial

July 26, 2013

Dear Col. Denise Lind,

On the night of July 25th I posted inappropriate messages on twitter relating to a hotel where I believed participants in the court martial of The United States v. Pfc. Bradley Manning were lodging. What I did was highly unprofessional. I am extremely embarrassed by my conduct and very sorry for my lapse of judgment.

This was the biggest mistake I've ever made in my life. I am deeply ashamed of this error. I deeply regret making this information known to the public. It was never my intention to cause any harm, intimidation, or confrontation; but I realize now how the message could be perceived in that manner.

My brother proudly served in the Army in Iraq in 2003 and 2004. I would be very upset if someone ever did this to him. Over the past couple years I have received over a dozen anonymous death threats related to my support of WikiLeaks and Bradley Manning, and I live every day fully understanding that intimidation, no matter how abstract, should never be taken lightly.

This afternoon, I deleted the tweets and I have refrained from sharing any details with the public and the press about what has happened.

Since December of 2011, I have been drawing the court martial proceedings, and I have been a proud member of the credentialed media since March of 2012 - attending nearly everyday. I have been hired to illustrate a book of the entire pretrial and trial. During the school year, I am an adjunct professor at Bloomfield College, in New Jersey, where I earn less than \$10,000 per year. This book is my livelihood and drawing the proceedings has been a dream-come true.

I beg you for your forgiveness. I cannot express enough how embarrassed and humbled I am by this lapse in judgment. I know in past years many famous people have made similar lapse in judgments on social media, and this situation has opened my eyes to my error, my lapse, and my wrongdoing.

I was informed that there are no specific rules, but that I was being removed at the decision of the Court. I understand this and know that I am in no position to ask for a second chance. Your Honor, I respect your Court, I respect your need for security and for decorum.

If you would reconsider this decision and allow me to return to Ft. Meade, to the media operations center but not the actual courtroom, I would be forever grateful. I would, of course, be on my best behavior both while at Ft. Meade and during my time off the base.

I am also writing a letter of apology that I hope to be able to send to those who I may have been affected by my tweet. My sincerest apologies to you and everyone involved in this most important proceeding.

Sincerely,

Clark Stoeckley

620a

PAGE

**Lind, Denise R COL USARMY (US)**

---

**From:** David Coombs [coombs@armycourt martialdefense.com]  
**Sent:** Friday, July 26, 2013 8:59 PM  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Bennett, Jessica D SSG USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Ellen, Alexander S (Alec) CPT USARMY (US); Mitroka, Katherine F CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); USARMY Ft McNair mdw Mailbox MDW Court Reporters OMB; Raffel, Michael J SFC USARMY (US); Moore, Katrina R MSG USARMY HQDA OTJAG (US); Fein, Ashley MAJ USARMY MDW (US)  
**Subject:** Clark Stoeckley  
**Attachments:** LetterofApology.pdf

Ma'am,

I wanted to inform the Court that I received the attached letter from Mr. Stoeckley. He also informed me that he sent this letter through PAO for you. After reading his letter, I believe that he deeply regrets his acts and would not repeat them. In light of this letter, I think the Court should consider allowing Mr. Stoeckley to return to either the media center or the courtroom.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government Response to  
Defense Motion for  
Reconsideration and for Mistrial:  
Specifications 4, 6, 8, 12, 16  
of Charge II  
(18 U.S.C. § 641 Offenses)

26 July 2013

### RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion for Reconsideration and for Mistrial: Specifications 4, 6, 8, 12, 16 of Charge II (18 U.S.C. § 641 Offenses) (hereinafter "Defense Reconsideration Motion").

### BURDEN OF PERSUASION AND BURDEN OF PROOF

"On request of any party or *sua sponte*, the military judge may, prior to authentication of the record of trial, reconsider any ruling, other than one amounting to a finding of not guilty, made by the military judge." Rule for Courts-Martial (hereinafter "RCM") 905(f). RCM 905(f) "permits the military judge to reconsider any ruling that affects the legal sufficiency of any finding of guilt or the sentence." RCM 905(f), discussion (citing RCM 917(d)).

"The military judge may, as a matter of discretion, declare a mistrial when such action is manifestly necessary in the interest of justice because of circumstances arising during the proceedings which cast substantial doubt upon the fairness of the proceedings." RCM 915(a).

### FACTS

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice (hereinafter "UCMJ"). The accused is also charged with causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, UCMJ, eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641 (hereinafter "§ 641"), two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications alleging misconduct in violation of Article 92 of the UCMJ. *See* Charge Sheet.

The accused pleaded guilty by substitutions and exceptions to Specifications 2, 3, 5, 7, 9, 10, 13, 14 and 15 of Charge II. *See* Appellate Exhibit (hereinafter "AE") CDXLIV. The accused did not plead guilty, *inter alia*, to Specifications 4, 6, 8, 12, and 16 of Charge II. *See id.*

### WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States requests that the Court consider the Charge Sheet, testimony, and the Appellate Exhibits (hereinafter "AE") cited herein.

APPELLATE EXHIBIT 621  
PAGE RE: ENCL: \_\_\_\_\_  
PAGE OF PAGES \_\_\_\_\_

## LEGAL AUTHORITY AND ARGUMENT

§ 641 reaches information as charged. The Defense had substantial notice as detailed herein and as explicitly acknowledged by the Defense prior to the start of the trial. Therefore, the Defense has not been prejudiced, and the Defense's request for reconsideration or a mistrial should be denied.

### I. DEFENSE ACKNOWLEDGED USE OF INFORMATION

The Defense had substantial notice that the United States intended to prove valuation by the contents—the information—in the asported records. *See* Government § 641 Response Part III.B (detailing numerous filings describing the expected testimony of Mr. Lewis regarding the value of information). The Defense avers that it would have conducted its case differently had it known information would be at issue. The United States has informed the Defense not only of the use of information in the charged property, but also of the use of contextual information outside the charged property. *See* AEDXLIV. The United States stated:

Similarly, valuation evidence also requires specialized knowledge appropriate for expert testimony. The United States will demonstrate valuation by presenting evidence of the information's value in a thieves' market. This opinion is based on unique, specialized knowledge and experience of an intelligence professional and is unknown to the average fact finder. The thieves' market requires demonstration of what types of information are valuable to foreign adversaries. The evidence is further strengthened by an explanation of why the information is valuable. Moreover, any type of evidence supporting valuation necessarily requires discussion of content and context. The thieves' market involves the motives and resources of foreign adversaries. Furthermore, the United States will present evidence about the systems required to create, maintain, and protect the information. This technical and financial information is also beyond the ken of an average fact finder. Thus, an expert is appropriate for presentation of valuation evidence and discussion of its context.

AEDXLIV. In response, the Defense acknowledged the appropriateness of the use of information, stating:

The Defense acknowledges that Government witnesses are permitted to testify as to alleged value of the information and to any alleged "thieves market" for the information. Since value is based upon face, par, or market value, these witnesses should be permitted to state how this information is valued. Establishing the alleged value (face, par, or market) of the charged information does not require the witness to testify about any information

beyond the four corners of the document. The "context" to the information within the charged document and how that information could or could not impact on other information is simply not relevant. The charged information has value, if at all, based upon its content and not based upon contextual information surrounding the document.

AE DXLVII (footnote omitted). Based on the arguments, the Court ruled that limited contextual information outside the charged property would be admissible. *See* AE DXLIX. Thus, information contained in the charged property is also properly admissible. *See* AE DCXIII.

Furthermore, the Defense argues that Mr. Lewis's testimony is prejudicial despite the filings described in Part III.B of the Government § 641 Response. Notwithstanding these filings and the Court stating it would permit the Defense to re-open its case to locate a valuation expert, the Defense did not request a Defense expert in counterintelligence. Moreover, the Defense also did not request to brief the issue of Mr. Lewis's expertise. Instead, the Defense cross-examined Mr. Lewis and fully litigated Mr. Lewis's expertise during the trial. The Defense raises no law in support of its position regarding Mr. Lewis. In lieu of precedent, the Defense attacks Mr. Lewis's credibility with an unsworn letter that has not been admitted into evidence. The Defense proffers this unsworn letter that discusses an issue about which Mr. Lewis was subject to cross-examination, *see* Testimony of Mr. Lewis, after Mr. Lewis's testimony and not at trial. In response to cross-examination by the Defense, Mr. Lewis distinguished between valuing a random document and valuing classified information; Mr. Lewis testified he could value classified information and accordingly offered an opinion on the value of the compromised information. *See id.*

## II. UNITED STATES CHARGED DATABASES CONTAINING RECORDS

The Defense asserts that it "did not know that either 'databases' or 'records' included information until 24 July 2013, after the close of evidence." Defense Reconsideration Motion at 1. This assertion repeats the same argument presented by the Defense in the Defense Motion for Directed Verdict: Charge II, Specifications 4, 6, 8, 12 (hereinafter "Defense § 641 Motion"). *See, e.g.,* Defense § 641 Motion ¶ 5. The United States briefed these issues in the Government Response to Defense Motion for Directed Verdict: Charge II, Specifications 4, 6, 8, 12, and 16 (hereinafter "Government § 641 Response") and the Government Brief on 18 U.S.C. § 641 and Intangible Property, to include Information. *See* AEDXCLXXXVI; AE DCVI.

Contrary to Defense arguments, the United States need not specifically allege information in the Charge Sheet. *See United States v. Fowler*, 932 F.2d 306, 309-10 (4th Cir. 1991). In *Fowler*, the Fourth Circuit upheld the defendant's conviction under § 641 for converting information where the defendant was charged with converting and conveying documents. *See id.* The Fourth Circuit noted that the accused "was not charged with conveying abstract information. He was charged with conveying and converting documents, which, although copies, were things of value and tangible property of the United States." *Id.* (deciding that § 641 applied to information). Similarly, the Third Circuit found merit to the argument that § 641 encompassed

information where the United States "charged that the defendants . . . converted to their own use 'records of the United States; that is, photocopies of official files of the Federal Bureau of Investigation, of a value in excess of \$100.00.'" *United States v. DiGilio*, 538 F.2d 972, 975-78 (3d Cir. 1976). Thus, the Third Circuit found information to be an inherent component of a record that need not be specifically charged where the accused had notice that he was charged with converting records. *See id.*; AE DCXIII.

Furthermore, courts use the terms "record" and "information" interchangeably. *See United States v. Jordan*, 582 F.3d 1239, 1246-47 (11th Cir. 2009). In *Jordan*, an accused was charged with conveying a "thing of value of the United States, that is, information contained in the NCIC records." *Id.* at 1246. The Eleventh Circuit used "record" and "information" interchangeably, and interpreted the § 641 charge as requiring the prosecution to prove that the defendant "knowingly and without authority conveyed a thing of value, a criminal record obtained from the NCIC, to [co-defendant], and that [co-defendant] knowingly received and retained it." *See id.* at 1247; *id.* at 1244 ("Count Two charged [defendant] with conveying the NCIC records to [co-defendant] . . . in violation of § 641."). A record inherently contains information. *See* AE DCXIII. Therefore, the United States was not required to charge "information" specifically where it charged a collection of records. *See* Charge Sheet.

The precedent cited by the Defense is inapplicable to this case. *United States v. Veloria*, 2011 WL 1330779 at \*4 (A. Ct. Crim. App. 2011), holds that substituting one owner of the property for another is a major amendment. Similarly, *United States v. Marshall*, 67 M.J. 418, 420-21 (C.A.A.F. 2009) holds that substituting the identity of the accused's custodian as charged constituted a material and, therefore, fatal variance. Here, the amendment approved by the Court, *see* AE DCXIII, does not substitute one property for another; rather, it reduces the scope of the charged property. *See* Government § 641 Response Part II.C. The database source of the charged records or the source of the stolen email accounts in the United States Forces-Iraq Global Address list has not been substituted. The sources remain the same. The amendments are minor and therefore permissible. *See id.*; AE DCXIII.

### III. VALUATION OF INFORMATION DOES NOT PREJUDICE DEFENSE

In accordance with the Court's ruling, *see* AE DCXIII, the United States relies on two forms of evidence of valuation. First, the United States relies on the expert opinion of Mr. Lewis. Second, the United States relies on evidence of the personnel costs required to create the records. The value of services used to create property is proper evidence of the property's value. *See United States v. May*, 625 F.2d 186, 192 (8th Cir. 1980) (holding that cost of pilot salaries was part of the value of converted flight time). Moreover, computer files have been valued by calculating the wages paid to create the files. *United States v. Walter*, 43 M.J. 879, 885 (N-M. Ct. Crim. App. 1996) ("The valuation method employed—the personnel or labor cost of producing or reproducing the files, was reasonable and conservative under the circumstances.").

Here, the United States presented evidence of the time required to create detainee assessment briefs and email accounts in the United States Forces-Iraq Global Address list. The evidence provides conservative estimates based on the most junior Soldiers and is therefore appropriate under *Walter*. *See Walter*, *supra*. Moreover, the valuation submitted by the United

States is based on the cost of creating the individual email account of detainee assessment briefs. Decreasing the number of email accounts does not affect the cost per account. Therefore, the minor amendment to Specification 16 of Charge II does not affect this evidence. The smaller number does not prejudice the accused because he is not subject to increased punishment, nor has the charged property changed outside a reduction in scope.

The Defense suffered no prejudice with evidence that documents are valued by their contents. See Government § 641 Response Part III. "Where documents constitute the property 'obtained or used,' as that phrase has been defined, the 'ideas' contained in the documents, rather than the paper on which the ideas are written, establish the value of the stolen property." *Diglio*, 538 F.2d at 977 n.9. To hold that records cannot be valued by their contents and intrinsic qualities "would do violence to the purpose statute." See *id.* at 979 (finding that payments made constituted proper evidence of value on a thieves market) (quoting *United States v. Lester*, 282 F.2d 750, 755 (3d Cir. 1960)). Indeed, "there must be some flexibility with respect to methods of proof of value." *Id.* (comparing market valuation under § 641 to valuation under 18 U.S.C. § 2313).

The Defense began its case by proffering that the accused selected specific types of records based on the information therein. The Defense proffered that: 1) significant activity reports from the Combined Information Database Network Exchanges Iraq and Afghanistan did not discuss future missions, 2) cables from the Net-Centric Diplomacy database did not contain intelligence sources, 3) detainee assessment briefs did not have intelligence sources listed by name, and 4) the accused selected the information to make the world a better place.

The United States briefed the Defense more than 18 months in advance of trial about the evidence and theory of this case. See AE CCLXIV Enclosures 4-5. The Defense was briefed about the digital forensic evidence the United States intended to use at trial. The Defense argument that it would have conducted its case differently, see Defense Reconsideration Motion ¶ 23, lacks merit. The Defense Reconsideration Motion demurs to its tactical decisions after-the-fact. Ultimately, the Defense admits it considered objecting to evidence but chose to waive these objections. See Government § 641 Response Part I.C. The Defense's current objections set forth in the Defense Reconsideration Motion are not timely and should be precluded accordingly.

#### IV. MISTRIAL INAPPROPRIATE

RCM 915(a) vests military judges with the discretion to declare a mistrial when "manifestly necessary in the interest of justice because of circumstances arising during the proceedings which cast substantial doubt upon the fairness of the proceedings." RCM 915(a). "However, the discussion to the rule advises caution, noting that mistrials are to be used 'under urgent circumstances, and for plain and obvious reasons.'" *United States v. Ashby*, 68 M.J. 108, 122 (C.A.A.F. 2009) (citing RCM 915, discussion). In the instant matter, the Defense had ample notice of the use of information and the United States' prosecutorial theory. Accordingly, the circumstances do not cast doubt upon the fairness of the proceedings. The circumstances do not warrant a mistrial. See AE DCXIII.



CONCLUSION

§ 641 reaches information as charged. The Defense had substantial notice as detailed herein and as explicitly acknowledged by the Defense prior to the start of the trial. Therefore, the Defense has not been prejudiced, and the Defense's request for reconsideration or a mistrial should be denied.

1h n 2k

ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 26 July 2013.

1h n 2k

ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel



DEPARTMENT OF THE ARMY  
US ARMY INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, UNITED STATES ARMY GARRISON  
4551 LLEWELLYN AVENUE, SUITE 5000  
FORT GEORGE G. MEADE, MARYLAND 20755-5000

REPLY TO  
ATTENTION OF:

29 JUL 2013

Office of the Garrison Commander

Mr. Clark Stoeckley  
Adjunct Professor  
Bloomfield College  
467 Franklin Street  
Bloomfield, New Jersey 07003

Dear Mr. Stoeckley:

Pursuant to the statutory authority of Title 18, Section 1382, United States Code, you are hereby prohibited from entering all areas of Fort George G. Meade. This bar order is effective upon your receipt of this letter, and will remain in effect until rescinded in writing.

This limited bar order is based on the following misconduct: On 25 July 2013, you made a series of postings on your Twitter account, <https://twitter.com/WikileaksTruck>, identifying the lodging location of the members of the prosecution team for U.S. v. PFC Bradley Manning court-martial being held at Fort George G. Meade, Maryland. You posted the link to the hotel on numerous occasions, along with threatening comments, for example: "I don't know how they sleep at night, but I do know where..." Your postings were threatening in nature, and targeted government officials.

As the Garrison commander, it is my inherent duty to maintain good order and discipline and to ensure a safe environment for everyone that resides and works on the installation. Your actions cause me great concern for the security of Fort George G. Meade. To prevent further security threats, you are not permitted to enter Fort George G. Meade until further notice.

If you are found within the limits of Fort George G. Meade, you will be detained by military police authorities and turned over to Federal officials for prosecution under Section 1382 of Title 18 of the United States Code.

This Federal statute is hereby quoted in its entirety for your information:

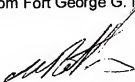
*Section 1382: Entering military, naval, or Coast Guard Property*

*Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation; or*

ATTACHMENT EXHIBIT 622  
PAGE 1 OF 1  
PAGE 1 OF 1 PAGES

*Whoever reenters or is found within any such reservation, post, fort, arsenal, yard, station, or installation, after having been removed therefrom or ordered not to reenter by any officer or person in command or charge thereof- shall be fined under this title or imprisoned not more than six months, or both.*

You have five (5) calendar days from the receipt of this letter to present me with matters as to why you should not be barred from Fort George G. Meade.



Edward C. Rothstein  
Colonel, U.S. Army  
Commanding

$y_0$ 

**RULING: Defense Motion  
For Reconsideration of  
Court's 24 July 2013 Supplemental  
Ruling – RCM 917 Motion  
18 U.S.C. §641 Specifications**

**30 July 2013**

The Defense Motion for Reconsideration presents additional argument for the issues raised in the original Defense Motion (AE 593). The Court adheres to its ruling at AE 613. The Court has ruled and the Defense has made its record.

The Defense Motion for Reconsideration is **DENIED**.

So **ORDERED** this 30th day of July 2013.

DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

**Verdict**

**Of Charge I and its specification – Not Guilty**

**Of Specification 1 of Charge II – Guilty**

**Of specification 2 of Charge II – in accordance with your plea, Guilty**, except the words and figures “15 February 2010” and “5 April 2010”, substituting therefore the words and figures “14 February 2010” and “21 February 2010”; further excepting the words “information relating to the national defense, to wit.”; further excepting the words “with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted,” substituting therefore the words “did willfully communicate”; further excepting the words and figures, “in violation of 18 U.S. Code Section 793(e),”; of the excepted words and figures, Not Guilty; of the substituted words and figures, Guilty.

**Of specification 3 of Charge II, Guilty** except the words and figures “22 March 2010”, substituting therefore the words and figures “17 March 2010”; of the excepted words and figures, Not Guilty, of the substituted words and figures, Guilty.

**Of specification 4 of Charge II, Guilty**

**Of specification 5 of Charge II, Guilty**

**Of specification 6 of Charge II, Guilty**

**Of specification 7 of Charge II, Guilty**

**Of specification 8 of Charge II, Guilty**

**Of specification 9 of Charge II, Guilty**

**Of specification 10 of Charge II, Guilty**

**Of specification 11 of Charge II, Not guilty**

**Of specification 12 of Charge II, Guilty**

**Of specification 13 of Charge II, Guilty**

**Of specification 14 of Charge II, in accordance with your plea, Guilty**, except the words and figures “15 February 2010” and “18 February 2010”, substituting therefore the words and figures “14 February 2010” and “15 February 2010”; further excepting the words “knowingly exceeded authorized access”, substituting therefore the words “knowingly accessed”; further excepting the words “with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)”; of the excepted words and figures, Not Guilty; of the substituted words and figures, Guilty.

**Of specification 15 of Charge II, Guilty**

**Of specification 16 of Charge II, Guilty**

**Of Charge II – Guilty**

**Of specification 1 of Charge III, Guilty**

**Of specification 2 of Charge III, Guilty**

**Of specification 3 of Charge III, Guilty**

**Of specification 4 of Charge III, Guilty**

**Of specification 5 of Charge III, in accordance with your plea, Guilty, except the words and figures "1 November 2009", substituting therefore the words and figures "8 January 2010"; of the excepted words and figures, Not Guilty; of the substituted words and figures, Guilty.**

**Of Charge III, Guilty**

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

SPECIAL FINDINGS

DATED: 15 August 2013

The Defense has requested the Court to issue special findings regarding the offenses for which the Court found PFC Manning guilty. The Court considered all legal and competent evidence, and the reasonable inferences to be drawn from the evidence, and resolved all issues of credibility. The Court will not make special findings for any specification where the finding was not guilty or guilty by exceptions and substitutions in accordance with PFC Manning's guilty plea.

The Court makes the following special findings:

**1. CHARGE II, Specification I: Wrongfully and Wantonly Causing Publication of Intelligence Belonging to the United States on the Internet Knowing the Intelligence is Accessible to the Enemy to the Prejudice of Good Order and Discipline in the Armed Forces or of a Nature to Bring Discredit Upon the Armed Forces**

1. The Court applied the following definitions for this offense:

"Intelligence" means any information helpful to the enemy which is true, at least in part.

"Enemy" includes not only organized opposing forces in time of war but also any other hostile body that our forces may be opposing and includes civilians as well members of military organizations.

"Wrongful" means without legal justification or excuse.

"Wanton" includes "recklessness" but may connote willfulness, or a disregard of probable consequences and thus describes a more aggravated offense. "Reckless" conduct is conduct that exhibits a culpable disregard of foreseeable consequences to others from the act or omission involved. PFC Manning need not intentionally cause a resulting harm. The ultimate question is whether under all the circumstances, PFC Manning's conduct was of that heedless nature that made it actually or imminently dangerous to others.

"Knowledge" requires that PFC Manning acted with actually knowledge that intelligence published on the internet was accessible to the enemy. The Court may not find the accused guilty of this offense if the Court finds PFC Manning should have known, but did not actually know this fact. Knowledge, like any other fact, may be proved by circumstantial evidence, including PFC Manning's training, experience, and military occupational specialty.

"Caused to be published" means the action of PFC Manning was a proximate cause of the publication even if it is not the only cause, as long as it is a direct or contributing cause that plays a material role,

meaning an important role, in bringing about the publication. An act is not a proximate cause if some other unforeseeable, independent, intervening event, which did not involve PFC Manning's conduct, was the only cause that played any important part in bringing about the publication.

"Conduct prejudicial to good order and discipline" is conduct which causes a reasonably direct and obvious injury to good order and discipline. "Service discrediting conduct" is conduct which tends to harm the reputation of the service or lower it in public esteem.

With respect to "prejudice to good order and discipline," the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as prejudicial in some indirect or remote sense; however, only those acts in which the prejudice is reasonably direct and palpable is punishable under this Article.

With respect to "service discrediting," the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as service discrediting in some indirect or remote sense; however, only those acts which would have a tendency to bring the service into disrepute or which tend to lower it in public esteem are punishable under this Article.

Under some circumstances, the accused's conduct may not be prejudicial to good order and discipline but, nonetheless, may be service discrediting. Likewise, depending on the circumstances, the accused's conduct can be prejudicial to good order and discipline but not be service discrediting.

2. The Court finds beyond a reasonable doubt that:

(1) at or near Contingency Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, PFC Manning wrongfully and wantonly caused to be published on the internet, intelligence belonging to the United States Government, having knowledge that Intelligence published on the internet is accessible to the enemy;

(2) the intelligence PFC Manning caused to be published on the internet included the 12 Jul 07 CZ Engagement Zone 30 GC Anyone.avi video charged in specification 2 of Charge II, the more than one classified memorandum produced by a United States government intelligence agency charged in specification 3 of Charge II, the more than 380,000 records from the Combined Information Data Network Exchange (CIDNE) Iraq database charged in specification 4 of Charge II, the more than 90,000 records from the CIDNE-A database charged in specification 6 of Charge II, the more than 700 records from the Southern Command (SOUTHCOM) database charged in specification 8 of Charge II, the more than five classified records relating to a military operation in Farah Province, Afghanistan charged in specification 10 of Charge II, the more than 250,000 cables from the Department of State Net-Centric Diplomacy database (DOS NCD) charged in specification 12 of Charge II, the classified DOS cable titled "Reykjavik-13" charged in specification 14 of Charge II, and the Army Counter-Intelligence Center (ACIC) Report dated 18 March 2008 entitled "Wikileaks.org-An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" charged in specification 15 of Charge II;

(3) At the time of the charged offense, al Qaeda and al Qaeda in the Arabian Peninsula were enemies of the United States. PFC Manning knew that al Qaeda was an enemy of the United States.

(4) At the time of the charged offense, PFC Manning had knowledge that intelligence published on the internet was accessible to al Qaeda.

(5) PFC Manning's conduct was wrongful.



(6) PFC Manning's conduct was of a heedless nature that made it actually and imminently dangerous to others. His conduct was both wanton and reckless.

(7) The conduct of PFC Manning was to the prejudice of good order and discipline in the armed forces.

(8) The conduct of PFC Manning was of a nature to bring discredit upon the armed forces.

**2. CHARGE II, Specifications 4, 6, 8, 12, and 16: Stealing, Purloining, or Knowingly Converting Records Belonging to the United States of a Value in Excess of \$1,000.00**

1. The Court applied the following definitions for these offenses:

To "steal" means to wrongfully take money or property belonging to the United States government with the intent to deprive the owner of the use and benefit temporarily or permanently.

"Wrongful" means without legal justification or excuse.

To "purloin" is to steal with the element of stealth, that is, to take by stealth the property of the United States government with intent to deprive the owner of the use and benefit of the property temporarily or permanently.

A "taking" doesn't have to be any particular type of movement or carrying away. Any appreciable and intentional change in the property's location is a taking, even if the property isn't removed from the owner's premises. PFC Manning did not have to know the United States government owned the property at the time of the taking.

A "conversion" may be consummated without any intent to permanently deprive the United States of the use and benefit of the property and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include the misuse or abuse of property. It may reach use in an unauthorized manner or to an unauthorized extent of property placed in one's custody for limited use. Not all misuse of government property is a conversion. The misuse must seriously and substantially interfere with the United States government's property rights.

"Value" means the greater of (1) the face, par, or market value, or (2) the cost price, whether wholesale or retail. A "thing of value" can be tangible or intangible property. Government information, although intangible is a species of property and a thing of value.

The market value of stolen goods may be determined by reference to a price that is commanded in the market place whether that market place is legal or illegal. In other words, market value is measured by the price a willing buyer will pay a willing seller. (The illegal market place is also known as a "thieves market".) "Cost price" means the cost of producing or creating the specific property allegedly stolen, purloined, or knowingly converted.

An act is done "willfully" if it is done voluntarily and intentionally with the specific intent to do something the law forbids, that is, with a bad purpose to disobey or disregard the law.

An act is done "knowingly" if it is done voluntarily and intentionally and not because of mistake or accident or other innocent reason.

The Court applies the same definitions for prejudice to good order and discipline in the armed forces and conduct of a nature to bring discredit upon the armed forces as applied in the special findings for specification 1 of Charge II.

The Court has taken judicial notice that Title 18, United States Code Section 641 was in existence on the dates alleged in specifications 4, 6, 8, 12, and 16 of Charge II.

2. The Court finds beyond a reasonable doubt that:

(1) at or near Contingency Operating Station Hammer, Iraq

**SPECIFICATION 4:** between on or about 31 December 2009 and on or about 5 January 2010; PFC Manning did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: a portion of the Combined Information Data Network Exchange Iraq database containing more than 380,000 records;

**SPECIFICATION 6:** between on or about 31 December 2009 and on or about 8 January 2010; PFC Manning did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: a portion of the Combined Information Network Exchange Afghanistan database containing more than 90,000 records;

**SPECIFICATION 8:** on or about 8 March 2010; PFC Manning did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: a United States Southern Command database containing more than 700 records;

**SPECIFICATION 12:** between on or about 28 March 2010 and on or about 27 May 2010; PFC Manning did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the Department of State Net-Centric Diplomacy database containing more than 250,000 records;

**SPECIFICATION 16:** between on or about 11 May 2010 and on or about 27 May 2010; PFC Manning did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: a portion of the United States Forces – Iraq Microsoft Outlook/SharePoint Exchange Server global address list (USF-I GAL), to wit: 74,000 addresses from the list.

(2) for specifications 4, 6, 8, 12, and 16 of Charge II, PFC Manning did steal and purloin the records, and information therein, by using the Secret Internet Protocol Router Network (SIPRnet) computers in the 2<sup>nd</sup> Brigade Combat Team, 10<sup>th</sup> Mountain Division (2/10<sup>th</sup> Bde) sensitive compartmented information facility (SCIF) to extract the records, and information therein, from the relevant database, place the records, and information therein, on PFC Manning's private portable digital media or platform, and asport the records, and information therein, to his private quarters. For specifications 4, 6, 8, 12, and 16 of Charge II, PFC Manning had the specific intent to steal at the time of the extraction of the records, and information therein, from the relevant database.

(3) for specifications 4, 6, 8, and 12 of Charge II, the Court finds that PFC Manning knowingly converted the records and information therein, by sending them to WikiLeaks. These knowing conversions involved a misuse of the records, and information therein, that seriously and substantially interfered with the United States government's property rights. The records, and information therein, are classified. The knowing conversions by PFC Manning deprived the United States government of the ability to protect its classified information by storing it only on classified networks required to be located

in a SCIF and by restricting access to the classified information only to persons with appropriate security clearances and a need to know the information.

(4) for specification 16 of Charge II, the Court finds PFC Manning specifically intended to knowingly convert the records, and information therein, by giving them to WikiLeaks. Following a pattern of stealing classified records, and information therein, and knowingly converting the classified records and information therein, to WikiLeaks, PFC Manning viewed a 7 May 2010 tweet from WikiLeaks requesting a list of as many .mil addresses as possible. PFC Manning drafted a tasker for himself to "acquire and exfiltrate Global Address List from United States Forces-Iraq (USF-I) Microsoft Outlook/Share-point Exchange server". PFC Manning used the peter.bigelow account on the 2/10<sup>th</sup> Bde supply room Non-secure Internet Protocol router Network (NIPRnet) computer to extract 74,000 email addresses that were part of the USF-I GAL. On or about 13 May 2013, PFC Manning asported the addresses to his personal Macintosh (MAC) computer, with the intent to send them to WikiLeaks. PFC Manning was apprehended on 27 May 2010. These acts were done with the specific intent to knowingly convert the records, and information therein, to WikiLeaks. The acts amounted to more than mere preparation. Preparation consists of devising or arranging the means or measures necessary for the commission of the attempted offense. They were a substantial step and a direct movement toward the commission of the knowing conversion. The acts would have apparently tended to bring about the commission of the intended offense of knowing conversion. The acts would have resulted in the actual commission of the offense of knowing conversion, except for the unexpected intervening circumstance of PFC Manning's apprehension on 27 May 2010, which prevented completion of that offense. Although not raised by the parties as a special defense, the Court finds that PFC Manning did not voluntarily abandon the attempted knowing conversion by deleting the 74,000 addresses on his MAC computer. PFC Manning deleted evidence of other classified information he knowingly converted to WikiLeaks from his personal MAC computer.

**(Special Findings Common to all specifications)**

(5) the records, and information therein, belonged to the United States or a department or agency, thereof;

(6) PFC Manning acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records; and

(7) the records were of a value greater than \$1,000.00 as valued by the cost of production of the information in the records and the records, and, as an independent basis of valuation for each specification, by the thieves market.

(8) at the time 18 U.S.C. Section 641 was in existence on the dates alleged in the specifications;

(9) under the circumstances, the conduct of PFC Manning was to the prejudice of good order and discipline in the armed forces.

(10) under the circumstances, the conduct of PFC Manning was of a nature to bring discredit upon the armed forces.

**3. CHARGE II, Specifications 3, 5, 7, 9, 10, and 15: Transmitting Defense information.**

1. PFC Manning's plea established all of the elements of these offenses except the following:

(1) the classified records, memorandum, video, and files described for each specification was information related to the national defense;

(2) PFC Manning had reason to believe the classified records, memorandum, video, and files described for each specification could be used to the injury of the United States or to the advantage of any foreign nation; and

(3) 18 U.S.C. §793(e) was in existence on the dates alleged in the specifications.

2. The Court applied the following definitions for these contested elements:

The term "national defense" is a broad term which refers to the United States military and naval establishments and to all related activities of national preparedness.

To prove that documents, writings, photographs, videos, or information relate to the national defense, there are two things that the government must prove:

- (1) that the disclosure of the material would be potentially damaging to the United States or might be useful to an enemy of the United States; and
- (2) that the material is closely held by the United States government, in that the relevant government agency has sought to keep the information from the public generally and has not made the documents, photographs, videos, or computer files available to the general public. Where the information has been made public by the United States government and is found in sources lawfully available to the general public, it does not relate to the national defense. Similarly, where the sources of information are lawfully available to the public, and the United States government has made no effort to guard such information, the information itself does not relate to the national defense.

In determining whether material is "closely held," the Court considered whether it has been classified by appropriate authorities and whether it remained classified on the date or dates pertinent to the charge sheet. The Court considered whether the information was classified or not in determining whether the information relates to the national defense. However, the fact that the information is designated as classified does not, in and of itself, demonstrate that the information relates to the national defense.

"Reason to believe" means that PFC Manning knew facts from which he concluded or reasonably should have concluded that the information could be used for the prohibited purposes. In considering whether PFC Manning had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign country, the nature of the information involved may be considered. The fact-finder need not determine that PFC Manning had reason to believe that the information would be used against the United States, only that it could be so used. Additionally, the likelihood of the information being used to the injury of the United States or to the advantage of any foreign nation must not be remote, hypothetical, speculative, far-fetched, or fanciful. The Government is not required to prove that the information obtained by PFC Manning was in fact used to the injury of the United States or to the advantage of any foreign nation.

The Government does not have to prove that PFC Manning had reason to believe that his act could both injure the United States and be to the advantage of a foreign country – the statute reads in the alternative. Also, the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

In determining whether the person who received the information was entitled to have it, the Court considered all the evidence introduced at trial, including any evidence concerning the classification status of the information, any evidence relating to law and regulations governing the classification and declassification of national security information, its handling, use, and distribution, as well as any evidence relating to regulations governing the handling, use, and distribution of information obtained from classified systems.

The Court has taken judicial notice that Title 18, United States Code Section 793(e) was in existence on the dates alleged in specifications 3, 5, 7, 9, 10, and 15 of Charge II.

3. The Court finds beyond a reasonable doubt as follows:

(1) **SPECIFICATION 3:** the more than one classified memorandum produced by a United States government intelligence agency was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States. The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**SPECIFICATION 5:** the more than 20 classified records from the Combined Information Data Network Exchange Iraq database was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States. The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**SPECIFICATION 7:** the more than 20 classified records from the Combined Information Data Network Exchange Afghanistan database was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States. The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**SPECIFICATION 9:** the more than 3 classified records from a United States Southern Command database was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States. The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**SPECIFICATION 10:** the more than 5 classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009 was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States. The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**SPECIFICATION 15:** the classified record produced by a United States Army intelligence organization, dated 18 March 2008 was information related to the national defense at the time of the willful communication. Disclosure of the material would be potentially damaging to the United States.

The more than one classified memorandum produced by a United States government intelligence agency was closely held by the United States government. PFC Manning had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.

**(Element Common to all specifications)**

(2) Title 18, United States Code Section 793(e) was in existence on the dates alleged in specifications 3, 5, 7, 9, 10, and 15 of Charge II;

(3) the conduct in specifications 5, 7, 9, 10, and 15 of Charge II occurred within the dates charged by the Government. The conduct in specification 3 of Charge II occurred within the dates charged by the Government as excepted and substituted by the Court in its verdict.

**3. CHARGE II, Specifications 13 - Fraud and Related Activity With Computers**

1. PFC Manning's plea established all of the elements of this offense except the following:

(1) PFC Manning knowingly exceeded authorized access on a Secret Internet Protocol Router Network Computer;

(2) PFC Manning had reason to believe such information so obtained, to wit: more than seventy-five classified United States Department of State (DOS) cables could be used to the injury of the United States or to the advantage of any foreign nation; and

(3) 18 U.S.C. §1030(a)(1) was in existence on the dates alleged in specification 13 of Charge II.

2. The Court applied the following definitions in accordance with the Court's Instructions and its 18 July 2012 Ruling: Defense Renewed Motion: Dismiss Specifications 13 and 14 of Charge II – Failure to State an Offense (AE 218):

The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

The term "exceeds authorized access" means that PFC Manning accessed a computer with authorization and used such access to obtain or alter information in the computer that PFC Manning is not entitled so to obtain or alter. It is the knowing use of the computer by exceeding authorized access which is being proscribed, not the unauthorized possession of, access to, or control over the protected information itself. Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can arise from a variety of sources to include regulations, user agreements, and command policies. Restrictions on access can include the manner of access.

The Court applied the same "Reason to believe" definition applied for specifications 3, 5, 7, 9, 10, and 15 of Charge II, violations of 18 U.S.C. §793(e) and Article 134, UCMJ.

The Court has taken judicial notice that Title 18, United States Code Section 1030(a)(1) was in existence on the date alleged in the specification.

3. The Court finds beyond a reasonable doubt as follows:

(1) Between on or about 28 March 2010 and on or about 27 May 2010, PFC Manning knowingly exceeded authorized access on a SIPRnet computer by knowingly introducing W-get, an unauthorized program to his user account on the DCGS-A SIPRnet computer he used in the 2/10th Bde SCIF and by using W-get to bypass the configured and authorized method of access and extraction of the seventy-five classified United States DOS cables from the NCD database. PFC Manning has expertise in automation and Department of Defense Information Security. He was placed on notice that W-get was an unauthorized program by Mr. Milliman prior to introducing W-get on the DCIGS-A computer. PFC Manning was required to sign an Acceptable Use Policy (AUP) similar to the example in AR 25-2, Appendix B. PFC Manning knew that Wget was not a game, music, or a movie. COL Miller tolerated games, music, and movies on the DCIGS-A computer to enhance morale. PFC Manning never inquired whether W-get was an authorized program on the DCIGS-A computer. Neither COL Miller nor anyone else in PFC Manning's supervisory chain told PFC Manning that W-get was an authorized program on the DCIGS-A computer.

(2) PFC Manning had reason to believe such information so obtained, to wit: more than seventy-five classified United States DOS cables could be used to the injury of the United States or to the advantage of any foreign nation; and

(3) 18 U.S.C. §1030(a)(1) was in existence on the dates alleged in specification 13 of Charge II.

**4. CHARGE III, Specifications 1-4: Violation of a Lawful General Regulation:**

1. The Court has taken judicial notice of AR 25-2, 24 October 2007.

2. The Court applied the following definitions to these offenses:

General regulations are those regulations which are generally applicable to an armed force and which are properly published by a military department.

PFC Manning may be found guilty of violating a general regulation only if the fact-finder is satisfied beyond a reasonable doubt that the regulation was a general regulation.

When a general regulation prohibits certain acts, except under certain conditions, then the burden is on the prosecution to establish by legal and competent evidence beyond a reasonable doubt that PFC Manning does not come within the terms of the exceptions.

3. The Court finds beyond a reasonable doubt the following:

(1) That there was in existence a certain lawful general regulation in the following terms:

**Specification 1:** paragraph 4-5(a)(4), Army Regulation 25-2, dated 24 October 2007;

**Specification 2:** paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;

**Specification 3:** paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;

**Specification 4:** paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;

(2) That PFC Manning had a duty to obey such regulation; and

(3) That at or near Contingency Operating Station Hammer, Iraq:

**Specification 1:** between on or about 1 November 2009 and on or about 8 March 2010, PFC Manning violated this lawful general regulation by attempting to bypass network or information security system mechanisms.

**Specification 2:** between on or about 11 February 2010 and on or about 3 April 2010, PFC Manning violated this lawful general regulation by adding unauthorized software, W-get, to a SIPRnet computer.

**Specification 3:** on or about 4 May 2010, PFC Manning violated this lawful general regulation by adding unauthorized software, W-get, to a SIPRnet computer.

**Specification 4:** between on or about 11 May 2010 and on or about 27 May 2010, PFC Manning violated this lawful general regulation by using an information system in a manner other than its intended purpose by extracting 74,000 email addresses from the USFI-GAL and by maintaining the email addresses on his private MAC computer.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit



## UNITED STATES

y.

**MANNING, Bradley E., PFC**

U.S. Army,

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall.

Fort Myer, VA 22211

**DEFENSE MOTION TO  
MERGE SPECIFICATIONS 5  
AND 7 OF CHARGE II FOR  
FINDINGS**

**DATED:** 30 July 2013

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 924(c), requests this Court to merge Specifications 5 and 7 of Charge II for findings.

2. "In a trial by military judge alone, the military judge may reconsider any finding of guilty at any time before announcement of sentence." R.C.M. 924(c).

3. The Government has conceded that the transmissions in Specifications 5 and 7 of Charge II were one transmission. The Court has previously stated that the Defense may make a motion to merge these specifications for findings after findings are announced. *See* Appellate Exhibit 78, Court Ruling on Defense Motion to Dismiss for Unreasonable Multiplication of Charges.

4. In light of the foregoing, the Defense requests this Court to merge Specifications 5 and 7 of Charge II for findings.

Respectfully submitted,

DAVID EDWARD COOMBS  
Civilian Defense Counsel

## UNITED STATES

 $\gamma_0$ 

**MANNING, Bradley E., PFC**

U.S. Army,

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall.

Fort Myer, VA 22211

**DEFENSE MOTION TO  
MERGE SPECIFICATIONS 4  
AND 6 OF CHARGE II FOR  
FINDINGS**

DATED: 30 July 2013

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 924(c), requests this Court to merge Specifications 4 and 6 of Charge II for findings.

2. "In a trial by military judge alone, the military judge may reconsider any finding of guilty at any time before announcement of sentence." R.C.M. 924(c).

3. The Government has conceded that the transmissions in Specifications 5 and 7 of Charge II were one transmission. The Court has previously stated that the Defense may make a motion to merge these specifications for findings after findings are announced. *See* Appellate Exhibit 78. Similarly, the taking of the information charged in Specifications 4 and 6 of Charge II, which is the subject of Specifications 5 and 7 of Charge II was one transaction. PFC Manning took these items at the same time. As such, the Defense requests that these specifications be merged as well for findings.

4. In light of the foregoing, the Defense requests this Court to merge Specifications 4 and 6 of Charge II for findings.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE MOTION TO  
MERGE AS UNREASONABLE  
MULTIPLICATION OF  
CHARGES FOR SENTENCING**

DATED: 30 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to *United States v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) and Rule for Courts Martial (R.C.M.) 1003(c)(1)(C), requests this Court find the below referenced specifications as an unreasonable multiplication of charges as applied to sentencing.

STANDARD

2. The military judge has the discretion to merge offenses "for sentencing purposes by considering the *Quiroz* factors and any other relevant factors that lead the military judge to conclude that the remedy of merger for sentencing is appropriate." *Campbell*, 71 M.J. at 24, citing *United States v. Quiroz*, 55 M.J. 334 (C.A.A.F. 2001).

FACTS

3. PFC Manning has been found guilty of five specifications of violating a lawful general regulation, three specifications of conduct prejudicial to good order and discipline and service discrediting, six specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and one specification of knowingly exceeding authorized access to a government computer, in violation of Articles 92 and 134 of the Uniform Code of Military Justice (U.C.M.J.) 10 U.S.C. §§ 892 and 934 (2010).

4. The Defense submits that the following four categories of specifications are an unreasonable multiplication of charges (UMC) as applied to sentencing:

Category 1: Article 134 (18 U.S.C. § 641) and Article 134 (18 U.S.C. § 793(e))

(A) Specifications 4 and 5 of Charge II involving the CIDNE-Iraq database containing more than 380,000 records belong to the United States government;

(B) Specifications 6 and 7 of Charge II involving the CIDNE-Afghanistan database containing more than 90,000 belonging to the United States government<sup>1</sup>;

(C) Specifications 8 and 9 of Charge II involving the United States Southern Command database containing more than 700 records belonging to the United States government;

Category 2: Article 134 (18 U.S.C. § 641) and Article 134 (18 U.S.C. § 1030(a)(1))

(A) Specifications 12 and 13 of Charge II involving the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States government;

Category 3: Article 134 (18 U.S.C. § 641 and 18 U.S.C. § 1030(a)(1)) and Article 92

(A) Specification 8 of Charge II involving the United States Southern Command database and Specification 2 of Charge III involving a violation of a lawful general regulation by adding unauthorized software to a Secret Internet Protocol Router Network computer;

(B) Specification 12 of Charge II involving the Department of State Net-Centric Diplomacy database and Specification 3 of Charge III involving a violation of a lawful general regulation by adding unauthorized software to a Secret Internet Protocol Router Network computer;

(C) Specification 16 of Charge II involving a portion of the United States Forces – Iraq Microsoft Outlook / Sharepoint Exchange Server Global Address List belonging to the United States government and Specification 4 of Charge III involving a violation of a lawful general regulation by using an information system in a manner other than its intended purpose.

DISCUSSION

5. The Court of Appeals for the Armed Forces (C.A.A.F.) in *United States v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) endorsed the following non-exclusive factors, commonly known as *Quiroz* factors, as a guide for military judges to consider when the defense objects to an UMC as applied to sentence:

- (1) Whether each charge and specification is aimed at distinctly separate criminal acts,
- (2) Whether the number of charges and specifications misrepresent or exaggerate the accused's criminality,

---

<sup>1</sup> The Defense has filed a motion to merge Specifications 4 and 6 of Charge II and also to merge Specifications 5 and 7 of Charge II for Findings.

- (3) Whether the number of charges and specifications unreasonably increase the accused's punitive exposure, or
- (4) Whether there is any evidence of prosecutorial overreaching or abuse in the drafting of the charges.

6. This Court has previously held pursuant to *Campbell* that:

None of the factors are pre-requisites. One or more factors may be sufficient to establish an UMC based on prosecutorial over-reaching. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. UMC may apply differently to findings than to sentencing. A charging scheme may not implicate the *Quiroz* factors in the same way that sentencing exposure does. In such a case, the nature of the harm requires a remedy that focuses more appropriately on punishment than findings.

See Appellate Exhibit (AE) 78, citing *Campbell*, 71 M.J. 23, 24.

7. Using the *Quiroz* factors, this Court should find that the above listed specifications of Charge II and III constitute an unreasonable multiplication of charges for sentencing. The Defense will address each category below:

a) Category 1: The listed specifications (4, 5, 6, and 7) involve conduct that essentially arose out of the same transaction and were part of the same impulse. These specifications are not aimed at distinctly separate criminal acts for sentencing purposes. In this case, PFC Manning took the CINDE-I and CIDNE-A SIGACTs on the same day. The taking of the SIGACTs was a necessary step in order to then subsequently give those SIGACTs to Wikileaks. The Government conceded the transmissions in Specifications 5 and 7 were one transmission. See AE 78. Additionally, the number of specifications misrepresents PFC Manning's criminality. The Government's charging decision takes a single ongoing act of removing SIGACTs and giving them to Wikileaks, and divides this conduct into four separate specifications. The dividing of this single act into four specifications takes what should be a ten year offense and makes it a forty year offense. The number of specifications unfairly increases PFC Manning's punitive exposure. Likewise, Specifications 8 and 9 involve conduct that arose out of the same transaction and was part of the same impulse. In order to give the records from the United States Southern Command database, PFC Manning had to take the records out of the T-SCIF. By dividing this ongoing act into two separate specifications, the Government takes what should be a ten year offense and makes it a twenty year offense and unfairly increases PFC Manning's punitive exposure.

b) Category 2: Specifications 12 and 13 involve conduct that arose out of the same transaction and was part of the same impulse. These specifications are not aimed at distinctly separate criminal acts for sentencing purposes. The taking of the records from the Department of State Net-Centric Diplomacy database was a necessary step in giving these records to Wikileaks. By dividing this ongoing act into two separate specifications, the Government takes what should

be a ten year offense and makes it a twenty year offense and unfairly increases PFC Manning's punitive exposure.

c) Category 3: Specifications 8 of Charge II and 2 of Charge III; 12 of Charge II and 3 of Charge III; and 16 of Charge II and 4 of Charge III involve either the use of unauthorized software or of an information system in order to take records from the United States Southern Command database, Department of State Net-Centric Diplomacy database, and the United States Forces – Iraq Microsoft Outlook / Sharepoint Exchange Server global address list. PFC Manning used the unauthorized software of Wget in order to obtain the records charged in Specifications 8 and 12 of Charge II. He also used an information system in a manner other than its intended purpose to obtain the records in Specification 16 of Charge II. These specifications are not aimed at distinctly separate criminal acts for sentencing purposes.

8. This Court should determine that: Specifications 4, 5, 6, and 7 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing; Specifications 8 and 9 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing; Specifications 12 and 13 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing; Specifications 8 of Charge II and 2 of Charge III; 12 of Charge II and 3 of Charge III; and 16 of Charge II and 4 of Charge III constitute an unreasonable multiplication of charges as applied to sentencing.

### CONCLUSION

9. For the reasons articulate above, this Court should determine the following:

a) that Specifications 4, 5, 6, and 7 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing and accordingly merge them into one specification;

b) that Specifications 8 and 9 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing and accordingly merge them into one specification;

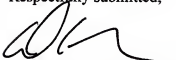
c) that Specifications 12 and 13 of Charge II constitute an unreasonable multiplication of charges as applied to sentencing and accordingly merge them into one specification;

d) that Specifications 8 of Charge II and 2 of Charge III; 12 of Charge II and 3 of Charge III; and 16 of Charge II and 4 of Charge III constitute an unreasonable multiplication of charges as applied to sentencing and accordingly merge the Charge III specifications into the Charge II specifications.

10. The current maximum punishment based upon the findings of the court is to be reduced to the grade of E-1; to total forfeitures of pay and allowances; to be discharged with a dishonorable discharge; and to be confined for a period of 136 years. Under the Defense's above request, the maximum punishment would be to be reduced to the Grade of E-1; to total forfeitures of pay and allowances; to be discharged with a dishonorable discharge; and to be confined for a period of 80

years.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'David E. Coombs', written over a horizontal line.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )  
Fort Myer, VA 22211 )

**DEFENSE MOTION FOR  
APPROPRIATE RELIEF  
UNDER R.C.M. 1001(b)(4)**

DATED: 31 July 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 1001(b)(4), requests this Court to limit the Government's sentencing evidence to its proper scope.

STANDARD

2. A military judge's decision to admit or exclude evidence is reviewed for an abuse of discretion. *United States v. Stephens*, 67 M.J. 233, 235 (C.A.A.F. 2009).

DISCUSSION

3. R.C.M. 1001(b)(4) permits trial counsel "to present evidence as to any aggravating circumstances directly relating to or resulting from the offenses of which the accused has been found guilty." Evidence in aggravation includes, but is not limited to, evidence of financial, social, psychological, and medical impact on or cost to any person or entity who was the victim of an offense committed by the accused and evidence of significant adverse impact on the mission, discipline, or efficiency of the command directly and immediately resulting from the accused's offense. *Id.*

4. "The phrase 'directly relating to or resulting from the offenses' imposes a 'higher standard' than 'mere relevance.'" *United States v. Rust*, 41 M.J. 472, 478 (C.A.A.F. 1995) (citing *United States v. Gordon*, 31 M.J. 30, 36 (C.M.A. 1990)). "Evidence is admissible on sentence which shows 'the specific harm caused by the defendant.'" *Id.* (quoting *Payne v. Tennessee*, 501 U.S. 808, 825 (1991)). "Nevertheless, an accused is not 'responsible for a never-ending chain of causes and effects.'" *Id.* (quoting *United States v. Witt*, 21 M.J. 638, 640 n.3 (A.C.M.R. 1985), *pet denied*, 22 M.J. 347 (C.M.A. 1986)). "Moreover, appellant's offense must play a material role in bringing about the effect at issue; the military judge should not admit evidence of an alleged consequence if an independent, intervening event played the only important part in



bringing about the effect.” *United States v. Fisher*, 67 M.J. 617, 621 (A. Ct. Crim. App. 2009)(quoting *United States v. Witt*, 21 M.J. 637, 640 (A.C.M.R. 1985).

5. As summarized in *United States v. Stapp*, 60 M.J. 795, 800-801 (A. Ct. Crim. App. 2004):

In sum, evidence of the natural and probable consequences of the offenses of which an accused has been found guilty is ordinarily admissible at trial. However, not every circumstance or consequence of misconduct may be admitted into evidence during the pre-sentencing portion of court-martial. An accused is not responsible for a never-ending chain of causes and effects. The standard for admission of evidence under this rule is not the mere relevance of the purported aggravating circumstance to the offense. A higher standard is required. The evidence sought to be admitted must establish that the offense of which appellant has been found guilty contributed to those effects which the government is trying to introduce in evidence. Moreover, appellant's offense must play a material role in bringing about the effect at issue; the military judge should not admit evidence of an alleged consequence if an independent, intervening event played the only important part in bringing about the effect. ... *cf.* Dep't of Army, Pam. 27-9, Legal Services: Military Judges' Benchbook, para. 5-19 (1 April 2001) (describing legal significance of intervening cause).

*Id.* (internal citations omitted). See also *United States v. Fisher*, 67 M.J. 617, 620-621 (A. Ct. Crim. App. 2009) (“...evidence in aggravation ... includes evidence of the natural and probable consequences of the offenses of which an accused has been found guilty, but not every circumstance or consequence of misconduct is admissible.... An accused is not responsible for a never-ending chain of causes and effects. The evidence sought to be admitted must establish that the offense of which appellant has been found guilty contributed to those effects which the government is trying to introduce in evidence.”) (internal citations omitted).

6. In *United States v. Hardison*, 64 M.J. 279, 281-282 (C.A.A.F. 2007), C.A.A.F. described the meaning of “directly related” for the purposes of R.C.M. 1001(b)(4):

The meaning of “directly related” under R.C.M. 1001(b)(4) is a function of both what evidence can be considered and how strong a connection that evidence must have to the offenses of which the accused has been convicted. Regarding the strength of the connection required between admitted aggravation evidence and the charged offense, this Court has consistently held that the link between the R.C.M. 1001(b)(4) evidence of uncharged misconduct and the crime for which the accused has been convicted must be direct as the rule states, and closely related in time, type, and/or often outcome, to the convicted crime. ... In regard to the strength of the connection needed, it is important to note that judicial discretion to admit uncharged misconduct under R.C.M. 1001(b)(4) was limited when the President promulgated the 1984 edition of the *Manual for Courts-Martial, United States* (1984 MCM), replacing the 1969 edition. The 1984 MCM replaced the original rule for the admission of evidence at sentencing, which allowed “any aggravating circumstances” with the requirement that the evidence in aggravation

be “directly related.” See *Manual for Courts–Martial, United States* (1969 rev. ed.).

7. Case law has consistently held that evidence offered under R.C.M. 1001(b)(4) must also pass the test of M.R.E. 403. See e.g. *United States v. Hardison*, 64 M.J. 279, 281-282 (C.A.A.F. 2007)(“The second limitation is that any evidence that qualifies under R.C.M. 1001(b)(4) must also pass the test of Military Rule of Evidence (M.R.E.) 403, which requires balancing between the probative value of any evidence against its likely prejudicial impact.”).

8. During the testimony of Brigadier General (BG) Robert Carr and Mr. John Kirchofer, the Defense objected under both relevance and R.C.M. 1001(b)(4) to three general areas of testimony that can be categorized as follows:

- (1) Chain of Events Testimony;
- (2) “Could” Cause Damage Testimony; and
- (3) Monetary Expenses and Use of Resources Testimony

The Defense believes that each of these general areas constitute impermissible testimony under R.C.M. 401; 1001(b)(4) and 403.

#### Chain of Events Testimony

9. BG Carr and Mr. Kirchofer’s testimony, as well as many of the Government’s other witnesses’ intended testimony, amounts to testimony of a never-ending chain of causes and effects, i.e. that due to PFC Manning’s conduct, a certain event happened that triggered another event that resulted in some remote harm. The testimony is nothing more than “when this happened, then that happened,” “when that happened, this other thing happened” and “when this other thing happened, yet a final thing happened.” PFC Manning is not responsible for a never-ending domino effect. Actions and activities of independent actors intervened in the meantime such that these fourth and fifth order effects cannot be said to be properly within the embrace of appropriate R.C.M. 1001 aggravation evidence. See *United States v. Rust*, 41 M.J. 472, 478 (C.A.A.F. 1995) (error to admit murder-suicide note where it cannot be said that murder was directly related to or resulting from the conduct of the appellant).

10. Moreover, if the Government were to be permitted to advance an attenuated chain of events that seek to place many of the ills of the world at PFC Manning’s feet, then the Court would have to allow the Defense to rebut this with evidence that PFC Manning’s disclosures actually effected meaningful change in the world. For instance, PFC Manning’s disclosures have been credited with empowering people in the Middle East and with precipitating “Arab Spring.” See <http://www.thedailybeast.com/articles/2013/06/03/how-bradley-manning-changed-the-war-on-terror.html> (“Some commentators have credited Manning’s leak with providing a spark for the revolutions that toppled the governments of Egypt and Tunisia and triggered uprisings in Bahrain, Libya, and Yemen, collectively known as the Arab Spring. Files leaked by Manning disclosed a secret relationship between the U.S. government and President Ali Abdullah Saleh of Yemen, to allow drone strikes inside the country where the United States was not in a declared war. Another cable detailed the private investments and holdings of the Tunisian ruling family.”). The Defense submits that allowing either the Government or the Defense to go down

this road would be improper aggravation or mitigation and would run afoul of R.C.M. 1001(b)(4) and R.C.M. 1001(c)(1)(B) respectively.

#### "Could" Cause Damage Testimony

11. BG Carr and Mr. Kirchofer testified as to how PFC Manning's misconduct "could" have caused damage. Specifically, they testified the information could have revealed TTPs; could have added to the knowledge of our adversary as to how much information that the United States knew or did not know; could have endangered individuals identified as sources for the United States; could have further traumatized family members of soldiers that were either killed or injured during combat due to being named in the released SIGACTs; could have impacted our information sharing down to the lower levels because superiors would no longer trust individuals at lower levels to protect classified information; and that the damage from PFC Manning's misconduct could have been much worse if it were not for the IRTF. The Defense objected to this testimony as not being relevant or proper under R.C.M. 1001(b)(4). The time for "could" cause damage testimony was during the merits phase of the trial. During sentencing, the witnesses should be limited to testimony regarding whether PFC Manning's conduct "did" cause damage.

12. If something "could" happen, that means that it "did not" happen. If it "did not" happen (but only "could" happen), by definition, it cannot be directly related to or resulting from the accused's conduct. In other words, something that is directly related to or resulting from the accused's conduct is something that *actually did happen*, not something that *could happen*.

13. A court would not countenance "could" evidence in sentencing in any case, nor would a trial counsel even attempt to offer "could" evidence in aggravation. For instance, if an accused is convicted of drinking and driving, a trial counsel would not offer evidence that the accused *could have* hurt someone; a trial counsel would offer evidence that an accused *did* hurt someone. In an adultery case, a trial counsel would not offer evidence that the accused *could have* caused damage to his family relationship; a trial counsel would offer evidence that an accused *did* cause damage to his family relationship. In an assault case, a trial counsel would not offer evidence that the accused *could have* caused a concussion; a trial counsel would offer evidence that an accused *did* cause a concussion. This case should be no different. The fact that this case involves classified evidence does not change what can properly be admitted in sentencing – i.e. what PFC Manning's actions *caused*, not what PFC Manning's actions *could have* caused.

14. In addition to offering the speculative potential damage, the Government attempted to smuggle inadmissible hearsay under the basis of the expert's opinion. The Defense objected to this testimony, and argued that the respective witnesses were "fact" witnesses and not "expert" witnesses. Additionally, the Defense argued that the Government was simply trying to admit inadmissible facts or data through BG Carr and Mr. Kirchofer. The Court determined that this type of information was not admissible under M.R.E. 703 unless the Court determined that the probative value in assisting the Court to evaluate the expert's opinion substantially outweighs the prejudicial effect of the inadmissible facts or data. The Defense maintains that the admission of inadmissible fact or data is improper under M.R.E. 703 since the probative value of the information does not substantially outweigh the prejudicial effect.

#### Monetary Expenses and Use of Resources Testimony

15. BG Carr and Mr. Kirchofer both testified about the formation of the IRTF. Mr. Kirchofer testified in greater detail about the monetary and human resources expended in setting upon the IRTF. Specifically, Mr. Kirchofer testified that the IRTF obtained 75 computers and over 125 personnel to work in reviewing the disclosed information. Mr. Kirchofer also testified that over 300 individuals transitioned through the IRTF during its 10 month existence. Finally, Mr. Kirchofer testified that the cost of the IRTF was approximately \$6.2 million. The Defense objected to this testimony as being improper under R.C.M. 1001(b)(4). The Defense argues that the monetary expenses and use of resources testimony was not directly related to or resulting from PFC Manning's misconduct since the expense of the IRTF was based upon an independent, intervening event – Secretary of Defense Robert Gates' decision to set up a task force to research the disclosures and determine what mitigation steps may be necessary. See *United States v. Fisher*, 67 M.J. 617, 621 (A. Ct. Crim. App. 2009)(testimony concerning the time devoted to appellant's court-martial and trial counsel's use of this evidence in sentencing argument was improper under R.C.M. 1001(b)(4)); *United States v. Stapp*, 60 M.J. 795, 800-801 (Army Ct. Crim. App. 2004)(military judge erred when he allowed a witness to testify concerning the effect of the court-martial itself upon the readiness of the company since the exercise of independent discretion to court-martial a soldier is not properly attributable to appellant as aggravation evidence).

16. The testimony from BG Carr and Mr. Kirchofer regarding monetary expenses and the use of resources is not directly related to or resulting from PFC Manning's conduct. The decision to create the IRTF was the result of the independent discretion of the Secretary Robert Gates. Secretary Gates established the IRTF in order to provide mitigation strategies, to identify insensitivities to religion or cultural beliefs with the releases, to research issues that might cause fractions with any coalition partner, and to provide notice of other possible releases. To provide an example of how this testimony is improper, assume an accused vandalized a building with spray paint. The costs of repainting the portion of the building vandalized would certainly qualify as proper aggravation under R.C.M. 1001(b)(4). However, if the owner of the building decided to repaint the whole building and hired an exterior designer to provide visual examples of how the building might look depending upon the color chosen, this expense would not be proper aggravation under R.C.M. 1001(b)(4). Similarly, if the building owner decided to expend significant resources in researching anti-graffiti paint options to avoid a future vandalism incident, such an expense would also not be proper aggravation under R.C.M. 1001(b)(4). In each instance, the cost of the designer and the cost of researching anti-graffiti paint would not be directly related to or resulting from the accused conduct since the act of the accused did not play a material role in bringing about the effect at issue. Instead, an independent, intervening event played the only important part in bringing about the effect – the owner decided to hire an exterior designer or research anti-graffiti paint. In the case at hand, the decision to establish the IRTF and to expend \$6.2 million was a result of an independent, intervening event and is not proper aggravation under R.C.M. 1001(b)(4).

17. The Defense anticipates that many of the remaining Government witnesses will also offer testimony that relates to the expenditure of financial or human resources. These witnesses will attempt to testify that these expenses were done as part of either the investigation of PFC Manning's misconduct or the organization's response to PFC Manning's misconduct. In either instance, the testimony is improper since it is not "the specific harm caused by the defendant."

*United States v. Rust*, 41 M.J. 472, 478 (C.A.A.F. 1995) (quoting *Payne v. Tennessee*, 501 U.S. 808, 825 (1991)).

CONCLUSION

18. In light of the foregoing, the Defense requests this Court to determine that the proffered chain of events testimony; "could" cause damage testimony; and monetary expenses and use of resources testimony is not proper aggravation evidence under R.C.M. 1001(b)(4). The Defense requests that the Court disregard the improper testimony offered by BG Carr and Mr. Kirchofer.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'DAVID EDWARD COOMBS', written over a horizontal line.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government Response  
to Defense Motion for  
Appropriate Relief Under  
RCM 1001(b)(4)

1 August 2013

RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion for Appropriate Relief Under RCM 1001(b)(4) (hereinafter "Defense Motion") because the accused's misconduct directly contributed to the matters described in the testimony of the United States' sentencing witnesses.

BURDEN OF PERSUASION AND BURDEN OF PROOF

"The trial counsel may present evidence as to any aggravating circumstances directly relating to or resulting from the offenses of which the accused has been found guilty. Evidence in aggravation includes, but is not limited to, evidence of financial, social, psychological, and medical impact on or cost to any person or entity who was the victim of an offense committed by the accused and evidence of significant adverse impact on the mission, discipline, or efficiency of the command directly and immediately resulting from the accused's offense." Rule for Courts-Martial (hereinafter "RCM") 1001(b)(4).

FACTS

The accused was convicted of causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, UCMJ, six specifications of misconduct in violation of 18 U.S.C. § 793(e), five specifications of misconduct in violation of 18 U.S.C. § 641, one specification of misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications of misconduct in violation of Article 92, UCMJ, and two specifications of conduct prejudicial to good order and discipline in violation of Article 134, UCMJ. See Appellate Exhibit (hereinafter "AE") DCXXIV.

WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States requests that the Court consider the testimony and Appellate Exhibits cited herein.

## LEGAL AUTHORITY AND ARGUMENT

### I. ACCUSED'S MISCONDUCT CONTRIBUTES TO AGGRAVATING CIRCUMSTANCES

The United States may present “evidence as to any aggravating circumstances directly relating to or resulting from the offenses of which the accused has been found guilty.” RCM 1001(b)(4); *see United States v. Zachary*, 61 M.J. 813, 819 (A. Ct. Crim. App. 2005) (stating that aggravating factors serve to increase the permissible punishment for a particular offense). Evidence in aggravation includes, *inter alia*, “significant adverse impact on the mission, discipline, or efficiency of the command” and impact or cost to any entity victimized by the accused’s offenses. *See* RCM 1001(b)(4); *see also United States v. Metz*, 34 M.J. 349, 351 (C.M.A.1992) (holding that uncharged conduct was admissible because it was “interwoven” in the *res gestae* of the crime and provided information to determine criminal intent).

Aggravating evidence that directly relates to the offenses is admissible. *See, e.g., United States v. Martin*, 20 M.J. 227, 232 (C.M.A. 1985) (citing *United States v. Vickers*, 13 M.J. 403 (C.M.A. 1982). The phrase “directly relating to or resulting from the offenses” imposes a “higher standard” than “mere relevance.” *See, e.g., United States v. Gordon*, 31 M.J. 30, 36 (C.M.A. 1990). Evidence that is “the natural and probable [consequence]” of the offense directly relates to the offense. *See United States v. Fisher*, 67 M.J. 617, 620 (A. Ct. Crim. App. 2009) (citing *United States v. Stapp*, 60 M.J. 795, 800 (A. Ct. Crim. App. 2004), *aff’d*, 64 M.J. 179 (C.A.A.F. 2006)). Consequential evidence is not admissible where “an independent, intervening event played the only important part in bringing about the effect.” *Id.* (citing *Stapp*, 60 M.J. at 800-01) (emphasis added). Consequential evidence that is closely related in time, type, or often outcome of the crime is admissible, *see United States v. Hardison*, 64 M.J. 279, 281-82 (C.A.A.F. 2007), because it establishes a reasonable linkage between the offense and the aggravating circumstances. *United States v. Witt*, 21 M.J. 637, 641 (A.C.M.R. 1985). A reasonable linkage exists where the offense “contributed” to the aggravating circumstances. *See id.* at 641 (finding neither a “but for” test nor facts sufficient to constitute proximate cause are required to establish a reasonable linkage, thus a reasonable linkage is a lesser standard than a “but for” and proximate cause test).

Aggravating evidence may be direct or circumstantial. *See United States v. Harrod*, 20 M.J. 777, 779 (A.C.M.R. 1985) (citing *United States v. Pooler*, 18 M.J. 832, 833 (A.C.M.R. 1984). Additionally, aggravating evidence may include the circumstances surrounding that offense or the repercussions of the offense itself, *see United States v. Gogas*, 58 M.J. 96, 98 (C.A.A.F. 2003) (quoting *Vickers*, 13 M.J. at 406) thereby enabling the sentencing authority to understand the gravity of the offense. *See United States v. Stebbins*, 61 M.J. 366, 373 (C.A.A.F. 2005). However, aggravating evidence is admissible only if its probative value outweighs its prejudicial effect. *See, e.g., United States v. Hursey*, 55 M.J. 34, 36 (C.A.A.F. 2001) (stating that sentencing evidence is subject to the balancing test under M.R.E. 403). The “military judge has wide discretion” in applying this balancing analysis. *See United States v. Yanke*, 23 M.J. 144 (C.M.A. 1987).



## II. EFFECT ON UNITED STATES GOVERNMENT IS PROPER AGGRAVATING EVIDENCE

The accused has been convicted of compromising over 700,000 United States Government documents. The accused compromised documents from multiple United States Government agencies; each of these agencies is an affected entity and a victim for national security purposes under RCM 1001(b)(4) where the effects are directly attributable to the accused's misconduct.

### A. Effects on National Security Are Proper Aggravation Evidence

RCM 1001(b)(4) presents illustrative examples that constitute a non-exhaustive list of potential aggravating evidence. See RCM 1001(b)(4) (stating that evidence in aggravation "is not limited to" the listed examples). The Drafters contemplated additional aggravating factors for the determination of punishment. See RCM 1004(c)(2)(A)-(C). In particular, the Drafters identified "knowingly creat[ing] a grave risk of substantial damage to the national security of the United States," or "knowingly creat[ing] a grave risk of substantial damage to a . . . function of the United States . . ." RCM 1004(c)(2)(B), or "caus[ing] substantial damage to the national security of the United States . . ." RCM 1004(c)(2)(A)-(C). RCM 1004(c)(2)(A)-(C) presents additional aggravating factors not explicitly listed in the non-exhaustive list of examples set forth in RCM 1001(b)(4). Although capital punishment is not at issue in this case, RCM 1004 serves as an illustrative example of the types of aggravating factors contemplated by the Drafters. Thus, the impact of the accused's misconduct on national security is properly admissible where it is connected to the accused's acts.

Impact may extend beyond the unit because that is but one type of aggravating evidence contemplated under RCM 1001(b)(4). See *United States v. Barber*, 27 M.J. 885 (A.C.M.R. 1989) (considering effect of blackmarketing in relation to the objectives of the Agreement on the Status of United States Armed Forces in Korea (SOFA)). In *Barber*, the Army Court of Military Review recognized that the "Army sends military forces into the sovereign nation of the Republic of Korea for mutually beneficial reasons of national security," and found a "reasonable linkage" between the accused's misconduct and the broader effects of blackmarketing on the victim entity, which was the command. See *id.* at 887. Here, the accused has been convicted of compromising hundreds of thousands of United States Government documents; the voluminous compromises had widespread effects, to include the formation of task forces and working groups, and causation of actual and potential harm to national security. Because the accused's misconduct caused these effects, they are directly related and admissible under RCM 1001(b)(4). Additionally, the impact of the accused's conduct extends beyond national security, and these impacts are also proper aggravating evidence under RCM 1001(b)(4). See, e.g., proffered testimony of Ambassador Kozak, see AE DV.

### B. Potential Harm Is Also Proper Aggravation Evidence

The accused's creation of risk and potential harm is proper aggravating evidence. See *United States v. Jones*, 44 M.J. 103, 104-105 (holding that subjecting the victim to risk of potential harm was admissible under RCM 1001(b)(4)); *United States v. Bauer*, 1999 WL



293907 at \*2 (A.F. Ct. Crim. App. 1999) (applying *Jones* to find no abuse of discretion by the military judge in instructing the members that they could consider potential damage to national security as an aggravating factor); *see also* RCM 1004(c)(2)(A)-(C). In particular, the risk to national security created by an intelligence analyst's misconduct aids understanding the circumstances surrounding the misconduct. *See Bauer* at \*2; *Jones*, 44 M.J. at 104 (upholding instruction for members to consider potential threat to national security where the accused, an intelligence analyst, was convicted of fraudulent enlistment, making a false official statement, and use of cocaine) (citing *United States v. Irwin*, 42 M.J. 479, 483 (C.A.A.F. 1995)). Furthermore, evidence of the scope of the criminal dissemination of unlawful information on the Internet constitutes evidence of potential harm that is proper aggravating evidence. *See United States v. Delgado*, 2013 WL 3238073 at \*3 (N-M. Ct. Crim. App. 2013) (concluding that distributing unlawful information to "countless unknown recipients" exacerbated "the grave nature of the crimes"); *cf. United States v. Pooler*, 18 M.J. 832, 833 (A.C.M.R. 1984) ("Evidence of the offender's attitude toward similar offenses, past or future, is reliable circumstantial evidence, and often the only available evidence, on this issue."). In *Delgado*, the widespread dissemination of the unlawful information onto the Internet created the potential for repetition of the crime, thus increasing the harm to the victims. *See Delgado, supra*.

In the instant case, the accused's misconduct created risk as opined by experts for the United States. *See, e.g.*, Testimony of BG (R) Carr; Testimony of Mr. Kirchhofer; Testimony of Ms. Dibble; Testimony of Mr. Feeley. This risk falls under RCM 1001(b)(4)'s permissive "any aggravating evidence directly relating to or resulting from the offenses of which the accused has been found guilty." RCM 1001(b)(4). The broad scope of the accused's misconduct effected wide-ranging consequences, which include risk to the United States and its national security. *See* Testimony of BG (R) Carr; Testimony of Mr. Kirchhofer; Testimony of Ms. Dibble; Testimony of Mr. Feeley.

### III. NON-CRIMINAL REVIEWS ARE PROPER AGGRAVATING EVIDENCE

Evidence pertaining to the "administrative burden of the court-martial process" is ordinarily not admissible under RCM 1001(b)(4) . . . " *United States v. Fisher*, 67 M.J. 617, 621 (A. Ct. Crim. App. 2009). "The processing of a case, at least up until referral, is solely within the government's control." *Id.* at 621 n.3. The United States is not offering evidence of the expenses and actions associated with United States Army CID, FBI, and Department of State Diplomatic Security Services Criminal Investigations, or costs associated with the accused's prosecution.

In this case, the national security task forces and working groups conducted by the United States Government to assess the consequences of the accused's misconduct fall outside this prohibition because these reviews were not conducted to determine criminal liability. *See United States v. Lonetree*, 35 M.J. 396, 403 (C.M.A. 1992) (holding that a damage assessment was not a criminal investigation for the purpose of determining whether the accused was entitled to an Article 31(b) warning because it was not coordinated with the criminal investigation); *see also* AE LXXII (differentiating between a damage assessment and criminal investigation); BATES Numbers 00504636-00504637 (stating that the Information Review Task force will review classified documents posted to WikiLeaks and that the review is "separate from, and unrelated

to, any criminal investigations of the leaked information").<sup>1</sup> These task forces and working groups were established to mitigate immediately the harm to individuals and national security caused by the accused. Moreover, costs incurred in the formation and execution of a review process resulting from an accused's misconduct are proper aggravating evidence. See *United States v. Lawson*, 33 M.J. 946, 959-60 (N.M.C.M.R. 1991) (holding proper admissibility evidence of search costs resulting from dereliction of duty). Indeed, the Defense concedes that costs associated with determining and repairing damage directly attributable to an accused's misconduct are proper aggravation evidence. See Defense Motion ¶ 16 ("The costs of repainting the portion of the building vandalized would certainly qualify as proper aggravation under R.C.M. 1001(b)(4).").

Here, the financial costs, lost opportunity costs, and resources expended to determine the extent and effects of the intentional release of classified information are proper aggravating evidence because they were not conducted with an eye toward prosecution. See Testimony of BG (R) Carr. The purpose of the reviews conducted by United States Government agencies was to determine what information had been compromised and not to collect evidence for a future prosecution. Thus, the reviews were not criminal investigations. See Testimony of BG (R) Carr; Testimony of Mr. Kirchhofer. The criminal investigations stemmed directly from the accused's misconduct and focused entirely on determining the criminality of the accused's misconduct. See Testimony of SA Mander; Testimony of SA Graham; Testimony of SA Smith; Testimony of SA Shaver. Therefore, the resources and their circumstances constitute admissible aggravating evidence under RCM 1001(b)(4).

Furthermore, the reviews are distinct from corrective action taken by the United States Government such as implementing a prohibition on burning a CD because that prohibition would prevent future misconduct and is therefore not related to the accused's misconduct. The Defense asserts that the United States will present evidence akin to "a never-ending domino effect." Defense Motion ¶ 9. The Defense further avers that the United States will offer this type of evidence:

However, if the owner of the building decided to repaint the whole building and hired an exterior designer to provide visual examples of how the building might look depending upon the color chosen, this expense would not be proper aggravation under R.C.M. 1001(b)(4). Similarly, if the building owner decided to expend significant resources in researching anti-graffiti paint options to avoid a future vandalism incident, such an expense would also not be proper aggravation under R.C.M. 1001(b)(4).

Defense Motion ¶ 16. In discovery litigation, the United States maintained that it would not present evidence of subsequent remedial measures to prevent future criminal acts similar to those of which the accused has been convicted because it is not proper aggravation evidence. Such acts are deliberate steps taken by the United States to prevent future acts, and thus are not proper

---

<sup>1</sup> BATES Numbers 00504636-00504637 constitute Appendix A to the Information Review Task Force Damage Assessment, of which the Court took judicial notice. See AE DLXXXVIII. Appendix A is a memorandum signed by Secretary of Defense Robert Gates.

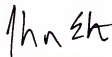
aggravation evidence in this matter. The United States made this determination that this type of information is not proper in response to litigation concerning the discovery of the Department of State "Mitigation Team" information. See AE CCXXII (noting that the "Mitigation Team" was established "to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of these documents").

#### IV. MRE 403 APPLICATION

Assuming, *arguendo*, the Court determines that the harm mitigation steps the United States Government took to prevent immediate harm to individuals, entities, and national security, are not proper aggravation evidence, the Defense should similarly be precluded from eliciting evidence regarding any absence of harm. If the Court determines that the United States Government's acts to mitigate harm are an independent and intervening event that played the only important part in bringing about the effect, then the Defense should be precluded from eliciting evidence of the effects of those acts—namely, the absence of harm. To present evidence of the absence of harm while simultaneously precluding evidence of steps to minimize harm would be unfairly prejudicial and misleading for the fact finder. Thus, the Defense should be precluded under Military Rule of Evidence 403 from eliciting such testimony and making related arguments.

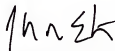
#### CONCLUSION

The United States respectfully requests that the Court deny the Defense Motion for Appropriate Relief Under RCM 1001(b)(4) because the accused's misconduct directly contributed to the matters described in the testimony of the United States' sentencing witnesses.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 1 August 2013.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel

## APPENDIX A

UNCLASSIFIED//FOR OFFICIAL USE ONLY



SECRETARY OF DEFENSE  
1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000

AUG 5 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
DIRECTOR, COST ASSESSMENT AND PROGRAM  
EVALUATION  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

Subject: Task Force to Review Unauthorized Disclosure of Classified Information (FOUO)

(U//FOUO) On July 28, 2010, I directed the Director, Defense Intelligence Agency (DIA) to establish an Information Review Task Force (IRTF) to lead a comprehensive Department of Defense (DoD) review of classified documents posted to the WikiLeaks website ([www.wikileaks.org](http://www.wikileaks.org)) on July 25, 2010, and any other associated materials. Department of Defense Components should provide DIA any assistance required to ensure the timely completion of the review.

(U//FOUO) The IRTF will review the impact of the unauthorized disclosure of classified information specified above. The IRTF will coordinate throughout the Intelligence Community in conducting this time-sensitive review and integrate its efforts with those of the National Counterintelligence Executive.

(U//FOUO) The IRTF will provide regular updates to the Office of the Secretary of Defense (OSD) on its findings. A more comprehensive interim report will be provided as the effort progresses. That report will include the following items:

- (U//FOUO) Any released information with immediate force protection implications;
- (U//FOUO) Any released information concerning allies or coalition partners that may negatively impact foreign policy;
- (U//FOUO) Any military plans;

OSD 09134-10



UNCLASSIFIED//FOR OFFICIAL USE ONLY

104

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) Any intelligence reporting;
- (U//FOUO) Any released information concerning intelligence sources or methods;
- (U//FOUO) Any information on civilian casualties not previously released;
- (U//FOUO) Any derogatory comments regarding Afghan culture or Islam; and
- (U//FOUO) Any related data that may have also have been released to WikiLeaks, but not posted.

A final report will be produced once all documents are assessed.

(U//FOUO) The IRTF is the single DoD organization with authority and responsibility to conduct the DoD review regarding this unauthorized disclosure. By separate tasking, I am directing USD(I) to conduct an assessment of the Department's procedures for accessing and transporting classified information.

(U//FOUO) This review is separate from, and unrelated to, any criminal investigation of the leaked information. The assessment and review of the leaked documents is not intended to, and shall not limit in any way, the ability of Department, Federal Bureau of Investigation or any other federal criminal investigators, trial counsel and prosecutors to conduct investigative and trial proceedings in support of possible prosecutions under the Uniform Code of Military Justice or federal criminal provisions.



cc:  
Director of National Intelligence  
Director, Central Intelligence Agency  
Assistant Secretary of State for Intelligence & Research  
National Counterintelligence Center

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Response to  
Defense Motion to Merge  
Specifications 5 and 7 of  
Charge II for Findings

2 August 2013

### RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion to Merge Specifications 5 and 7 of Charge II for Findings (hereinafter the "Defense Motion") under Rule for Courts-Martial (hereinafter "RCM") 924(c) because the application of the *Quiroz* factors for findings makes merger an inappropriate remedy. However, the United States does not object to merging these specifications for sentencing.

### BURDEN OF PERSUASION

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. *See* RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. *See* RCM 905(c)(2). Here, the defense bears this burden.

### FACTS

The accused was convicted of causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, Uniform Code of Military Justice (hereinafter "UCMJ"), six specifications of misconduct in violation of 18 U.S.C. § 793(e), five specifications of misconduct in violation of 18 U.S.C. § 641, one specification of misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications of misconduct in violation of Article 92, UCMJ, and two specifications of conduct prejudicial to good order and discipline in violation of Article 134, UCMJ. *See* Appellate Exhibit (hereinafter "AE") 624.

### WITNESSES/EVIDENCE

The United States does not request any witnesses or evidence be produced for this motion. The United States requests that the Court consider the evidence adduced at trial and the referenced Appellate Exhibits.

### LEGAL AUTHORITY AND ARGUMENT

The Court of Appeals for the Armed Forces (hereinafter "CAAF") in *United States v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) endorsed the following non-exclusive factors, commonly known as *Quiroz* factors in light of *United States v. Quiroz*, 55 M.J. 334, 339 (C.A.A.F. 2001),

AP EXHIBIT 632  
PAGE REFERENCE:  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

as a guide for military judges to consider when the defense objects that the United States has unreasonably multiplied the charges:

- (1) Whether each charge and specification is aimed at distinctly separate criminal acts;
- (2) Whether the number of charges and specifications misrepresent or exaggerate the accused's criminality;
- (3) Whether the number of charges and specifications unfairly increase the accused's punitive exposure; and
- (4) Whether there is any evidence of prosecutorial overreaching or abuse in the drafting of the charges.

See *Campbell*, 71 M.J. at 24. None of the *Quiroz* factors are pre-requisites, meaning one or more factors may be sufficient to establish an unreasonable multiplication of charges (hereinafter "UMC") based on prosecutorial over-reaching. See *Quiroz*, 55 M.J. at 339. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. See AE 78.

The CAAF in *Campbell* recognized that "the concept of UMC may apply differently to findings than to sentencing." *Campbell*, 71 M.J. at 23. When merging charges for sentencing purposes, the Court instructed military judges, in their discretion, to employ the above *Quiroz* factors and any other relevant factors as to whether merger for sentencing is appropriate. *Id.* at 24 n.9; RCM 1003(c)(1)(C) discussion; *United States v. Anderson*, 68 M.J. 378, 386 (C.A.A.F. 2010) (stating that "the application of the *Quiroz* factors involves a reasonableness determination, much like sentence appropriateness"); *Quiroz*, 55 M.J. at 399 (stating that the concept of UMC for sentencing applies "when the military judge...determines that the nature of the harm requires a remedy that focuses more appropriately on punishment than on findings").

Under Specifications 5 and 7 of Charge II, the accused was convicted of having unauthorized possession of more than 40 classified Significant Activities (hereinafter "SIGACTs") from the Combined Information Data Network Exchange (hereinafter "CIDNE") Iraq and Afghanistan databases, and transmitting those classified records to WikiLeaks. See Charge Sheet. The parties agree that the accused transmitted the SIGACTs from both databases at the same time. See Defense Motion, at ¶ 3. **Although the transmissions occurred at the same time, the crimes are separate because the crimes began on different days and the stolen property resided on different databases.** See discussion, *infra*. Additionally, the evidence adduced at trial proved that these specifications are aimed at separate and distinct criminal acts. Nevertheless, since the accused transmitted these SIGACTs at the same time, these specifications should merge for sentencing. See *Quiroz*, 55 M.J. at 399 (stating that the concept of UMC for sentencing applies "when the military judge...determines that the nature of the harm requires a remedy that focuses more appropriately on punishment than on findings").

**I: The evidence adduced at trial relating to the accused's unauthorized possession of the SIGACTs from the CIDNE Iraq and CIDNE Afghanistan databases demonstrate that these specifications aim at separate and distinct criminal acts.**

The evidence proved that the accused gained possession of the SIGACTs from their respective databases in very different ways. As an intelligence analyst in Iraq, the accused was connected to a server for the CIDNE Iraq database, making those SIGACTs contained therein readily accessible to him. *See* Prosecution Exhibit (hereinafter "PE") 116. On the other hand, the accused did not have ready access to the SIGACTs from the CIDNE Afghanistan database because Servicemembers deployed to Iraq, including members of the accused's unit, were not connected to a server for the CIDNE Afghanistan database. *See id.* Rather, the main servers to the CIDNE Afghanistan database were located throughout Afghanistan, and the back-up server was located at the United States Central Command Headquarters in Tampa, Florida. *See id.* Therefore, to possess the SIGACTs from the CIDNE Afghanistan database, the accused took it upon himself to connect to the back-up server in Tampa, Florida. The accused connected to the back-up server in Tampa from 1-7 January 2010. *See* PE 152. For Specification 6 of Charge II, the evidence proved that the accused, on 7 January 2010, between 11:51:30Z and 11:52:27Z (Zulu time), completed exporting more than 90,000 SIGACTs from the CIDNE-A database. *See id.*

SA Shaver testified that he found a password-protected folder named "yada.tar.bz2.nc" on the accused's personal computer. *See* Testimony of SA Shaver. This folder was created using "MCrypt", which SA Shaver testified is an open source utility to encrypt files that was found on the accused's personal computer. *See id.* Four files were located within the "yada.tar.bz2.nc" folder, one of which was entitled "irq\_events.csv" and another was entitled "afg\_events.csv." The file "irq\_events.csv" contained more than 380,000 SIGACTs from the CIDNE Iraq database. *See id.* The file "irq\_events.csv" was last written on 5 January 2010, which means 5 January 2010 was the last time the file "irq\_events.csv" was written to or updated on his personal computer. *See id.* The file "afg\_events.csv" contained more than 90,000 SIGACTs from the CIDNE Afghanistan database. The file "afg\_events.csv" was last written on 8 January 2010, meaning the last time that file was written to or updated on his personal computer was 8 January 2010. *See id.*

Simply put, the accused completed the theft of the SIGACTs from the CIDNE Iraq database on 5 January 2010, thus this date marks the beginning of the unauthorized possession for Specification 4 of Charge II. Three days later, on 8 January 2010, the accused completed the theft of the SIGACTs from the CIDNE Afghanistan database thus this date marks the beginning of the unauthorized possession for Specification 6 of Charge II. Further, his theft of the SIGACTs from the CIDNE Afghanistan database required the accused to take overt acts to connect to the CIDNE Afghanistan database, a database that does not share information with the CIDNE Iraq database. The accused stole the records employing different methods, from different databases, and on different days. The theft of the SIGACTs from the CIDNE Iraq database consists of distinctly separate criminal acts than the theft of the SIGACTs from the CIDNE Afghanistan database.

The accused gained possession of the SIGACTs from the CIDNE databases in very different ways. Further, the accused had unauthorized possession of the SIGACTs from the CIDNE Iraq database three days prior to his unauthorized possession of the SIGACTs from the CIDNE Afghanistan database. Although the accused eventually combined the records and



transmitted these records to WikiLeaks at the same time, the criminal acts leading up to this transmission highlight that these specifications are aimed at separate and distinct acts.

Two specifications carrying a maximum punishment of 20 years for the transmission of more than 40 classified SIGACTs from the CIDNE Iraq and CIDNE Afghanistan databases neither misrepresent or exaggerate the accused's criminality, nor unfairly increase the accused's punitive exposure. Under Specifications 5 and 7 of Charge II, the accused has been convicted of transmitting more than 40 classified SIGACTs to WikiLeaks. Put another way, the accused is facing a maximum punishment of one year confinement for every two classified documents he compromised. This does not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure – particularly since the criminal statute under which the accused was convicted, 18 U.S.C. § 793(c), criminalizes the unauthorized disclosure of one classified document for a maximum sentence of ten years. Further, the evidence adduced at trial proved that the CIDNE Afghanistan records transmitted by the accused have been in the possession of the enemies of our nation. The combined maximum punishment for these specifications, 20 years, accurately reflects the gravity and scope of the convicted offenses of transmitting more than 40 classified SIGACTs to an unauthorized person.

II: Since the accused transmitted the SIGACTs from the CIDNE Iraq and CIDNE Afghanistan database at the same time, the United States does not object to the merging of these specifications for sentencing.

Although the CAAF in *Campbell* noted that “[a]s a matter of logic and law, if an offense is multiplicitous for sentencing it must necessarily be multiplicitous for findings as well[,]” the Court further recognized how “the concept of unreasonable multiplication of charges may apply differently to findings than to sentencing.” *Id.* at 23. The Court explained that courts may implicate the *Quiroz* factors differently to the charging scheme than to sentencing exposure. *See id.* at 23. The evidence adduced at trial supports that these specification merge for sentencing, not for findings. The evidence proved that the accused downloaded the SIGACTs from the CIDNE Iraq database four days prior to downloading those from the CIDNE Afghanistan database. The evidence also proved that the accused was in unauthorized possession of the SIGACTs from the CIDNE Iraq database three days prior to having unauthorized possession of those from the CIDNE Afghanistan database. Nevertheless, since the accused transmitted the SIGACTs from both databases at the same time, the remedy should focus more on the accused's punitive exposure, which would be more proper for sentencing. *See Quiroz*, 55 M.J. at 399 (the concept of UMC for sentencing applies “when the military judge...determines that the nature of the harm requires a remedy that focuses more appropriately on punishment than on findings”).

#### CONCLUSION

The United States respectfully requests that the Court deny the Defense Motion because the application of the *Quiroz* factors for findings makes merger an inappropriate remedy. However, since the accused transmitted these records at the same time, the United States does not object to the merging of these specifications for sentencing.



J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 2 August 2013.



J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Response to  
Defense Motion to Merge  
Specifications 4 and 6 of  
Charge II for Findings

2 August 2013

### RELIEF SOUGHT

The United States respectfully requests that the Court deny the Defense Motion to Merge Specifications 4 and 6 of Charge II for Findings (hereinafter the "Defense Motion") under Rule for Courts-Martial (hereinafter "RCM") 924(c) because the application of the *Quiroz* factors makes merger an inappropriate remedy.

### BURDEN OF PERSUASION

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. *See* RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. *See* RCM 905(c)(2). Here, the defense bears this burden.

### FACTS

The accused was convicted of causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, Uniform Code of Military Justice (hereinafter "UCMJ"), six specifications of misconduct in violation of 18 U.S.C. § 793(e), five specifications of misconduct in violation of 18 U.S.C. § 641, one specification of misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications of misconduct in violation of Article 92, UCMJ, and two specifications of conduct prejudicial to good order and discipline in violation of Article 134, UCMJ. *See* Appellate Exhibit (hereinafter "AE") 624.

### WITNESSES/EVIDENCE

The United States does not request any witnesses or evidence be produced for this motion. The United States requests that the Court consider the evidence adduced at trial and the referenced Appellate Exhibits.

### LEGAL AUTHORITY AND ARGUMENT

The Court of Appeals for the Armed Forces (hereinafter "CAAF") in *United States v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) endorsed the following non-exclusive factors, commonly known as *Quiroz* factors in light of *United States v. Quiroz*, 55 M.J. 334, 339 (C.A.A.F. 2001), as a guide for military judges to consider when the defense objects that the United States has unreasonably multiplied the charges:

- (1) Whether each charge and specification is aimed at distinctly separate criminal acts;

- (2) Whether the number of charges and specifications misrepresent or exaggerate the accused's criminality;
- (3) Whether the number of charges and specifications unfairly increase the accused's punitive exposure; and
- (4) Whether there is any evidence of prosecutorial overreaching or abuse in the drafting of the charges.

See *Campbell*, 71 M.J. at 24. None of the *Quiroz* factors are pre-requisites, meaning one or more factors may be sufficient to establish an unreasonable multiplication of charges (hereinafter "UMC") based on prosecutorial over-reaching. See *Quiroz*, 55 M.J. at 339. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. See AE 78.

I: Specifications 4 and 6 of Charge II are aimed at distinctly separate criminal acts.

For Specification 4 of Charge II, the evidence proved that the accused, an intelligence analyst deployed to Iraq, had ready access to the Significant Activities (hereinafter "SIGACTs") from the Combined Information Data Network Exchange (hereinafter "CIDNE") Iraq database. With such access, the accused completed exporting more than 380,000 SIGACTs from the CIDNE Iraq database between 04:39:13C and 04:54:04C (Iraq time) on 3 January 2010. See Prosecution Exhibit (PE) 116.

For Specification 6 of Charge II, the evidence proved that the accused did not have ready access to the SIGACTs from the CIDNE Afghanistan database because Servicemembers deployed to Iraq, including members of the accused's unit, were not connected to a server for the CIDNE Afghanistan database. Rather, the main servers to the CIDNE Afghanistan database were located throughout Afghanistan, and the back-up server was located at the United States Central Command Headquarters in Tampa, Florida. See *id.* Therefore, to possess the SIGACTs from the CIDNE Afghanistan database, the accused took it upon himself to connect to the back-up server in Tampa, Florida. The accused connected to the back-up server in Tampa from 1-7 January 2010. See PE 152. On 7 January 2010, between 11:51:30Z and 11:52:27Z (Zulu time), the accused completed exporting more than 90,000 SIGACTs from the CIDNE-A database. See *id.*

SA Shaver testified that he found a password-protected folder named "yada.tar.bz2.nc" on the accused's personal computer. See Testimony of SA Shaver. This folder was created using "MCrypt", which SA Shaver testified is an open source utility to encrypt files that was found on the accused's personal computer. See *id.* Four files were located within the "yada.tar.bz2.nc" folder, one of which was entitled "irq\_events.csv" and another was entitled "afg\_events.csv." The file "irq\_events.csv" contained more than 380,000 SIGACTs from the CIDNE Iraq database. See *id.* The file "irq\_events.csv" was last written on 5 January 2010, which means 5 January 2010 was the last time the file "irq\_events.csv" was written to or updated on his personal computer. See *id.* The file "afg\_events.csv" contained more than 90,000 SIGACTs from the CIDNE Afghanistan database. The file "afg\_events.csv" was last written on 8 January 2010, meaning the last time that file was written to or updated on his personal computer was 8 January 2010. See *id.*

Simply put, the accused completed the theft of the SIGACTs from the CIDNE Iraq database on 5 January 2010. *Three days later*, on 8 January 2010, the accused completed the

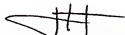
theft of the SIGACTs from the CIDNE Afghanistan database. Further, his theft of the SIGACTs from the CIDNE Afghanistan database required the accused to take overt acts to connect to the CIDNE Afghanistan database, a database that does not share information with the CIDNE Iraq database. The accused stole the records employing different methods, from different databases, and on different days. The theft of the SIGACTs from the CIDNE Iraq database consists of distinctly separate criminal acts than the theft of the SIGACTs from the CIDNE Afghanistan database.

II: Two specifications carrying a maximum punishment of 20 years for the theft of nearly 500,000 SIGACTs from the CIDNE Iraq and CIDNE Afghanistan databases neither misrepresent or exaggerate the accused's criminality, nor unfairly increase the accused's punitive exposure.

Under Specifications 4 and 6 of Charge II, the accused has been convicted of stealing nearly 500,000 SIGACTs. The sheer volume of data supports not merging these offenses. *See* AE 78 at 5 (concluding that the sheer volume of records weighs this *Quiroz* factor in favor of not merging the offenses). To steal these records, the accused exported SIGACTs from the CIDNE databases on 144 separate occasions. *See* PE 116 (stating that a user can export data from the CIDNE database *only* one month at a time). Further, the evidence adduced at trial proved that the SIGACTs from the CIDNE Afghanistan database transmitted by the accused have been in the possession of the enemies of our nation. *See* PE 153. The combined maximum punishment for these specifications, 20 years, accurately reflects the gravity and scope of the convicted offenses the accused's theft of nearly 500,000 SIGACTs.

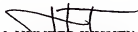
#### CONCLUSION

The United States respectfully requests that the Court deny the Defense Motion because application of the *Quiroz* factors makes merger an inappropriate remedy.



J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 2 August 2013.



J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Response to  
Defense Motion to Merge  
as Unreasonable Multiplication  
of Charges for Sentencing

2 August 2013

#### RELIEF SOUGHT

The United States respectfully requests that the Court deny, in part, the Defense Motion to Merge as Unreasonable Multiplication of Charges for Sentencing (hereinafter the "Defense Motion"). The United States agrees with the defense that Specification 16 of Charge II and Specification 4 of Charge III should merge into a single, ten-year offense for sentencing. However, for the remaining specifications which the defense requests that this Court merge, except for Specifications 5 and 7 of Charge II which are addressed in a separate filing, the application of the *Quiroz* factors makes merger an inappropriate remedy.

#### BURDEN OF PERSUASION

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. *See* RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. *See* RCM 905(c)(2). Here, the defense bears this burden.

#### FACTS

The accused was convicted of causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, Uniform Code of Military Justice (hereinafter "UCMJ"), six specifications of misconduct in violation of 18 U.S.C. § 793(e), five specifications of misconduct in violation of 18 U.S.C. § 641, one specification of misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications of misconduct in violation of Article 92, UCMJ, and two specifications of conduct prejudicial to good order and discipline in violation of Article 134, UCMJ. *See* Appellate Exhibit (hereinafter "AE") 624.

#### WITNESSES/EVIDENCE

The United States does not request any witnesses or evidence be produced for this motion. The United States requests that the Court consider the evidence adduced at trial and the referenced Appellate Exhibits.

#### LEGAL AUTHORITY AND ARGUMENT

The Court of Appeals for the Armed Forces (hereinafter "CAAF") in *United States v. Campbell*, 71 M.J. 19 (C.A.A.F. 2012) endorsed the following non-exclusive factors, commonly

APPELLATE EXHIBIT 634  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_\_ OF \_\_\_\_\_ PAGES

known as the *Quiroz* factors in light of *United States v. Quiroz*, 55 M.J. 334, 339 (C.A.A.F. 2001), as a guide for military judges to consider when the defense objects that the United States has unreasonably multiplied the charges:

- (1) Whether each charge and specification is aimed at distinctly separate criminal acts;
- (2) Whether the number of charges and specifications misrepresent or exaggerate the accused's criminality;
- (3) Whether the number of charges and specifications unfairly increase the accused's punitive exposure; and
- (4) Whether there is any evidence of prosecutorial overreaching or abuse in the drafting of the charges.

See *Campbell*, 71 M.J. at 24. None of the *Quiroz* factors are pre-requisites, meaning one or more factors may be sufficient to establish an unreasonable multiplication of charges (hereinafter "UMC") based on prosecutorial over-reaching. See *Quiroz*, 55 M.J. at 339. A singular act may implicate multiple and significant criminal law interests, none necessarily dependent upon the other. See AE 78.

The CAAF in *Campbell* recognized that "the concept of UMC may apply differently to findings than to sentencing." *Campbell*, 71 M.J. at 23. When merging charges for sentencing purposes, the Court instructed military judges, in their discretion, to employ the above *Quiroz* factors and any other relevant factors as to whether merger for sentencing is appropriate. *Id.* at 24, n.9; RCM 1003(c)(1)(C) discussion; *United States v. Anderson*, 68 M.J. 378, 386 (C.A.A.F. 2010) (stating that "the application of the *Quiroz* factors involves a reasonableness determination, much like sentence appropriateness"); *Quiroz*, 55 M.J. at 399 (stating that the concept of UMC for sentencing applies "when the military judge...determines that the nature of the harm requires a remedy that focuses more appropriately on punishment than on findings").

I. This Court should not merge the specifications of 18 U.S.C. § 641 violations with those of 18 U.S.C. § 793(e) violations, specifically Specifications 4 and 5 of Charge II, Specifications 6 and 7 of Charge II, or Specifications 8 and 9 of Charge II (collectively the "Category 1 Specifications"), for sentencing purposes because each of the *Quiroz* factors makes merger an inappropriate remedy.

Each of the *Quiroz* factors makes merger of the Category 1 Specifications an inappropriate remedy. The criminal acts in the Category 1 Specifications are separate and distinct, and the number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.

A. *The theft of the records in Specifications 4, 6, and 8 of Charge II and the transmission of those records in Specifications 5, 7, and 9 of Charge II are aimed at separate and distinct criminal acts.*

For Specification 4 of Charge II, the evidence proved that, in early January 2010, the accused began exporting the Significant Activities (hereinafter "SIGACTs") spanning six years from the Combined Information Data Network Exchange (hereinafter "CIDNE") Iraq database in

30-day increments. *See* PE 116 (stating that a user can export data from the CIDNE database *only* one month at a time). Put another way, the accused manually exported the CIDNE Iraq SIGACTs on 144 separate occasions. The accused completed exporting more than 380,000 SIGACTs from the CIDNE-I database between 04:39:13C and 04:54:04C (Iraq time) on 3 January 2010.

SA Shaver testified that he found a password-protected folder named “yada.tar.bz2.nc” on the accused’s personal computer. *See* Testimony of SA Shaver. This folder was created using “MCrypt”, which SA Shaver testified is an open source utility to encrypt files that was found on the accused’s personal computer. *See id.* Four files were located within the “yada.tar.bz2.nc” folder, one of which was entitled “irq\_events.csv.” The file “irq\_events.csv” contained more than 380,000 SIGACTs from the CIDNE Iraq database. *See id.* The file “irq\_events.csv” was last written on 5 January 2010, meaning the last time the file was written to or updated was 5 January 2010. *See id.*

For Specification 5 of Charge II, the evidence proved that, on 30 January 2010, the accused created the above folder entitled “yada.tar.bz2.nc” where he stored the file containing more than 380,000 SIGACTs from the CIDNE Iraq database. *See* Testimony of SA Shaver. Prior to forensically wiping his personal computer on 31 January 2010, the accused transmitted those records to WikiLeaks. *See* Testimony of Mr. Johnson; PE 125.

For Specification 6 of Charge II, the evidence proved that the accused completed exporting more than 90,000 SIGACTs from the CIDNE Afghanistan database between 11:51:30Z and 11:52:27Z (Zulu time) on 7 January 2010. *See* PE 116. The accused manually exported the CIDNE Afghanistan SIGACTs in 30-day increments on 144 separate occasions. *See* PE 116 (stating that a user can export data from the CIDNE database *only* one month at a time). SA Shaver testified that one of the files contained within the “yada.tar.bz2.nc” folder was named “afg\_evtnts.csv.” *See* Testimony of SA Shaver. The file “afg\_events.csv” contained more than 90,000 SIGACTs from the CIDNE Afghanistan database. The file “afg\_events.csv” was last written on 8 January 2010, meaning the last time the file was written to or updated was 8 January 2010. *See id.*

For Specification 7 of Charge II, the evidence proved that, on 30 January 2010, the accused created the above folder entitled “yada.tar.bz2.nc” where he stored the file containing more than 90,000 SIGACTs from the CIDNE Afghanistan database. *See id.* Prior to forensically wiping his personal computer on 31 January 2010, the accused transmitted those records to WikiLeaks. *See* Testimony of Mr. Johnson; PE 125.

For Specification 8 of Charge II, the evidence proved that, upon returning from leave on 5 March 2010, the accused unsuccessfully attempted to manually download the Detainee Assessment Briefs (hereinafter “DABs”) from the United States Southern Command (hereinafter “USSOUTHCOM”) database. *See* PE 82; *see also* Testimony of SA Shaver (testifying that the accused attempted to download the DABs using a right-click save method as an ordinary user on 5 March 2010 and that the code “000” on PE 82 means that the download was unsuccessful). Two days later, on 7 March 2010, the accused downloaded more than 700 DABs from the



USSOUTHCOM database with the software, WGET. See PE 83; Testimony of SA Shaver. The accused subsequently transferred the records to his personal computer.

For Specification 9 of Charge II, the evidence proved that the accused inquired about how valuable the DABs would be to WikiLeaks, to which he was told "quite valuable." See PE 123 at 5-6. Knowing that, on 8 March 2010, the accused then transmitted those records to WikiLeaks. See PE 123 at 5-6.

The defense, for the second time, argues the theft was a "necessary step" for the accused to transfer those records to WikiLeaks. See Defense Motion, at ¶ 7(a); see also AE 78, at 5 (noting the "defense argument that each violation of 18 U.S.C. § 641 was simply the 'first step' in a violation of 18 U.S.C. § 793(e)"). As previously foreclosed by this Court, this argument "has been discounted by the appellate courts in the context of larceny and false claims convictions." *Id.* (citing *United States v. Chatman*, 2003 WL 25945959 (A.C.C.A. 2003) (unpublished)). Appellate courts continue to discount this argument for sentencing purposes. See *United States v. Roosa*, 2013 WL 1850867 at 2-3 (A.C.C.A. 2013) (upholding the military judge's decision not to merge a larceny offense with a false claim offense for sentencing because "larceny is separate and distinct from [the appellant's] false claim, as collecting unauthorized funds from the United States requires a specific intent to permanently deprive").

In *Roosa*, the appellant was charged with stealing thousands of dollars by submitting fraudulent travel vouchers that reflected inflated lodging expenses based on fabricated lease agreements. At trial, the defense counsel requested to merge the larceny charge, false claim charge, and conduct unbecoming charge relating to the use of a co-worker's personal information for the purpose of sentencing. Instead, the military judge merged the false official statement charges with the conduct unbecoming charges. On appeal, the appellant sought to merge the larceny charge, false claim charge, and conduct unbecoming charge relating to the use of a co-worker's personal information on the fabricated lease agreements. The appellate court denied, *inter alia*, the request to merge the conduct unbecoming charge with the other charges because "[a]lthough the use of her co-worker's personal information formed part of the foundation for the false claim, this specification addressed the separate act of involving an unwitting partner in a criminal enterprise, and therefore reflects a distinct set of activities." *Id.* at 3. Similarly, here, although stealing the records may have eventually formed part of the foundation for the subsequent transmission, both acts reflect a distinct set of activities. See *id.*

During pretrial proceedings, this Court held that the Category 1 Specifications allege separate and distinct acts. See AE 78, at 5 (finding that "[t]he 18 U.S.C. § 641 offenses are aimed at the theft of government property...while the gravamen of the 18 U.S.C. § 793(e) offenses is the transmittal of national defense information to unauthorized persons"). This Court correctly reasoned that, as in the *Campbell* case, "the crime of theft of government records can be complete whether or not the accused willfully 'communicated...[or] transmitted' the records to persons not entitled to receive them." *Id.* at 5.

The CAAF also declines to find charges of distinct criminal acts multiplicitous, even where the acts, as a whole, represent a singular act. See *Campbell*, 71 M.J. at 22. In *Campbell*, the appellant was a nurse who was convicted of entering fraudulent physician orders into a

machine that dispensed medication and then stealing that medication. The appellant was convicted of falsely stating that he had a physician's order, wrongful possession of that medication, and larceny. The defense counsel requested that the military judge merge the possession charge with the larceny charge *for findings*, which the judge denied. On appeal, the Court affirmed that the criminal acts were separate and distinct for findings, and reasoned as follows:

In essence, the transactions at the [dispensing] machine may have each represented a singular act, *but each implicated multiple and significant criminal law interests*, none necessarily dependent on the others. For instance, in this case the evidence showed that Appellant falsely indicated in the [dispensing] machine that he had the proper authority to retrieve the particular medication when in fact he had no such authority. This offense was complete whether or not Appellant actually had the machine dispense the medication. Also, theoretically, after indicating he had proper authority and after forming the requisite specific intent to steal, Appellant could nonetheless have changed his mind regarding his intent to steal after the machine dispensed the medications. He could, at that point, have decided to turn the medications over to proper authority and avoided wrongfully possessing the property.

*Id.* at 24-5 (emphasis added). Similarly, here, the accused could have stolen the SIGACTs and then he could have chosen not to transmit them to WikiLeaks.

In *Campbell*, the military judge did merge the above offenses *for sentencing*. The military judge reasoned that the false official statement, larceny, and wrongful possession "essentially arose out of this same transaction and were part of the same impulse." *Id.* at 22. Here, the accused's theft and transmission did not arise out of the same transaction and certainly were not part of the same impulse. In *Campbell*, the criminal acts forming the basis of the three offenses all took place in a short amount of time, consecutive to one another. The appellant entered the fraudulent physician's order into the dispensing machine, which promptly dispensed medication into his wrongful possession.

Here, for Specification 4 of Charge II charging violations of 18 U.S.C. § 641, the evidence proved that the accused completed manually exporting more than 380,000 SIGACTs from the CIDNE-I database on 3 January 2010. For Specification 6 of Charge II, the accused completed exporting more than 90,000 SIGACTs from the CIDNE-A database on 7 January 2010. SA Shaver testified that he found a file entitled "irq\_events.csv" on the accused's personal computer contained more than 380,000 SIGACTs from the CIDNE Iraq database. *See id.* The file "irq\_events.csv" was last written on 5 January 2010, which means 5 January 2010 was the last time the file "irq\_events.csv" was written to or updated on his personal computer. *See id.* SA Shaver testified that he found a file entitled "afg\_events.csv" containing more than 90,000 SIGACTs from the CIDNE Afghanistan database. The file "afg\_events.csv" was last written on 8 January 2010, meaning the last time that file was written to or updated on his personal computer was 8 January 2010. *See id.*

For Specifications 5 and 7 of Charge II charging violations of 18 U.S.C. § 793(e), the evidence proved that the accused transmitted the records originating from two separate and distinct classified databases to WikiLeaks prior to forensically wiping his personal computer on 31 January 2010. *See* Testimony of Mr. Johnson; PE 125.

For Specification 8 of Charge II, the evidence proved that the accused stole the records on 7 March 2010 after unsuccessfully attempting to download the DABs two days earlier. For Specification 9 of Charge II, after confirming with Julian Assange that the DABs would be valuable, the accused transmitted the records to WikiLeaks.

Unlike in *Campbell*, here, the offenses at issue did not take place concurrently or in a matter of seconds. Instead, the evidence proved that the accused stole the records and, *days later*, eventually transmitted the records to WikiLeaks. *See* PE 30 (admitting to Adrian I.amo that he sorted and compressed the data before transmitting it to WikiLeaks). Further, the accused formed a separate criminal intent for the theft offenses than for the transmission offenses.

Further, the theft and transmission are not part of one transaction. In *Roosa*, the military judge merged the conduct unbecoming charge relating to the use of a co-worker's personal information in a fabricated lease agreement with the false official statement charge relating to signing fabricated lease agreements for sentencing. *See Roosa*, 2013 WL 1850867, at 2. The fabricated lease agreement included the co-worker's personal information, thereby consisting of one transaction for UMC purposes for sentencing. Here, the theft and the transmission are not part of one transaction. Instead, the accused stole the records and then engaged in a separate criminal act when he later chose to transmit those records to WikiLeaks.

B. *The number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.*

The CAAF in *Campbell* upheld the military judge's decision to merge the offenses for sentencing because not doing so "might have exaggerated Appellant's criminal and punitive exposure in light of the fact that, from Appellant's perspective, he had committed one act implicating three separate criminal purposes." *Id.* at 25. Here, in contrast with *Campbell*, the number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure. The accused has been convicted of stealing nearly 500,000 SIGACTs from two separate and distinct classified databases and then, days later, transmitting several of those classified records to WikiLeaks. The sheer volume of data supports not merging these offenses. *See* AE 78, at 5 (concluding that the sheer volume of records weighs this *Quiroz* factor in favor of not merging the offenses). To steal these records, the accused exported SIGACTs from the CIDNE databases on 144 separate occasions. Further, the evidence adduced at trial proved that the records transmitted by the accused have been in the possession of the enemies of our nation. The accused's criminal acts are far more serious, both in scope and gravity, than those in *Campbell*. The combined maximum punishment for these specifications, 40 years, accurately reflects the gravity and scope

of the accused's theft of nearly 500,000 SIGACTs from two separate and distinct classified databases and then, days later, transmitting several of those classified records to WikiLeaks.

II. This Court should not merge Specifications 12 and 13 of Charge II (collectively the "Category 2 Specifications") for sentencing purposes because each of the *Quiroz* factors makes merger an inappropriate remedy.

Each of the *Quiroz* factors makes merger of the Category 2 Specifications an inappropriate remedy. The criminal acts in the Category 2 Specifications are separate and distinct, and the number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.

*A. The evidence adduced at trial proved that the theft of the records in Specification 12 of Charge II and the subsequent transmission of those records in Specification 13 of Charge II are aimed at separate and distinct criminal acts.*

For Specification 12 of Charge II, the evidence proved that, from 28 March 2010 to 9 April 2010, the accused connected to the Department of State firewall more than 700,000 times. *See* PE 159. During this time, the accused employed WGET to download more than 250,000 cables from the Net-Centric Diplomacy (hereinafter "NCD") database webserver. *See* Testimony of SA Shaver (testifying that the accused stored an automated WGET script used to download cables from the NCD database webserver on the accused's SIPRNET computer). On 28 March 2010, the accused systematically began stealing the downloaded cables by transferring them, in batches, to his personal computer. *See* PE 127, lines 36-48. The accused completed his theft of more than 250,000 cables on 10 April 2010. *See id.*, at line 48.

After stealing the cables, the accused sorted and compressed the data into a Comma Separated Value (hereinafter "CSV") file, and encoded the cables in Base64 format, which compacts the data and makes it easier to transport. *See* Testimony of Mr. Johnson (testifying that the accused stored a script on his personal computer that he used to convert information from a cable into Base64 CSV format); *see also* Testimony of SA Shaver (testifying that the CSV format makes it easier to move around data and Base64 compacts the data); *see also* PE 30 (admitting to Adrian Lamo that he sorted and compressed the data before transmitting it to WikiLeaks). Then, the accused transmitted those cables to WikiLeaks.

During the pretrial stage, this Court held that the Category 2 Specifications allege separate and distinct acts. *See* AE 78, at 6 (finding that "[t]he 18 U.S.C. § 641 offense is aimed at the theft of government property...while the 18 U.S.C. § 1030(a)(1) offense requires the transmittal of classified information to unauthorized persons"). This Court correctly reasoned, as in the *Campbell* case, that the crime of theft of government records can be complete whether or not the accused willfully transmitted the records to persons not entitled to receive them. *Id.*, at 6.

The evidence adduced at trial proved that the accused's theft of more than 250,000 cables is separate and distinct from his subsequent transmission. The accused stole the cables over a two week period, from 28 March 2010 to 10 April 2010. After stealing the cables, the accused packaged and catalogued the cables. Afterwards, the accused chose to transmit those cables to

WikiLeaks. As stated above, although the theft may have eventually formed part of the foundation for the subsequent transmission, both acts reflect a distinct set of activities. *See Roosa*, 2013 WL 1850867 at 3.

*B. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.*

The number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure. The accused has been convicted of stealing more than 250,000 Department of State cables from a classified database and transmitting several of those classified records to WikiLeaks. The sheer volume of data supports not merging these offenses. *See* AE 78, at 5 (concluding that the sheer volume of records weighs this *Quiroz* factor in favor of not merging the offenses). Further, the evidence adduced at trial proved that a portion of the cables transmitted by the accused have been in the possession of the enemies of our nation. *See* PE 153(a). The combined maximum punishment for these specifications, 20 years, accurately reflects the gravity and scope of the convicted offenses of stealing more than 250,000 cables from a classified database and transmitting those records to WikiLeaks.

III. This Court should not merge Specification 8 of Charge II with Specification 2 of Charge III or Specification 12 of Charge II and Specification 3 of Charge III (collectively "Category 3 Specifications") for sentencing purposes because each of the *Quiroz* factors makes merger an inappropriate remedy.

Each of the *Quiroz* factors makes merger of the Category 3 Specifications an inappropriate remedy. The criminal acts in the Category 3 Specifications are separate and distinct, and the number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.

*A. The evidence adduced at trial proved that the theft of the records in Specifications 8 and 12 of Charge II and the regulatory violations in Specifications 2 and 3 Charge III, respectively, are aimed at separate and distinct criminal acts.*

For Specification 8 of Charge II and Specification 2 of Charge III, the evidence proved that, sometime before 7 March 2010, the accused added unauthorized software, WGET, to his SIPRNET computer. After adding WGET to his SIPRNET computer, the accused then had to learn how to program WGET to operate. *See* Testimony of SA Shaver. The accused downloaded the WGET help output file to determine how to operate WGET. *See id*; *see also* PE 189. The accused also searched how to make WGET operate faster, *after* he unsuccessfully attempted to manually download the DABs on 5 March 2010. *See* PE 157. On 7 March 2010, the accused downloaded more than 700 DABs from the USSOUTHCOM database and subsequently transferred the records to his personal computer. The act of adding WGET to his SIPRNET computer and the act of stealing DABs are separate and distinct. Army Regulation 25-2 criminalizes the act of introducing unauthorized software on a SIPRNET computer; the purpose being to protect the information system. That offense was committed when the accused uploaded WGET onto his computer sometime before 7 March 2010. But then, after adding

WGET to his computer, the accused had to learn how WGET operated and what script to write to steal the DABs. Specification 8 of Charge II criminalizes the act of stealing United States Government property; the purpose being to protect government property. Although adding WGET to his computer may have eventually formed part of the foundation for the subsequent theft, it was the accused's use of WGET that ultimately led to the theft. *See Campbell*, 71 M.J. at 24-25 (recognizing that a singular act may implicate multiple and significant criminal interests not dependent on the others).

For Specification 12 of Charge II, as explained above, the accused stole more than 250,000 cables over a two week period, from 28 March 2010 to 10 April 2010. *See supra*. Specification 3 of Charge III, on the other hand, relates to when the accused re-introduced WGET to his SIPRNET computer in early May 2010. *See Charge Sheet*. In early May 2010, after stealing more than 250,000 cables one month earlier, the accused returned to the NCD database to download the remaining cables from March 2010 forward. *See* PE 159 (showing that the accused connected to the Department of State firewall more than 53,000 times on 3 May 2010). The accused catalogued these additional cables in a file entitled "backup.xlsx," which was created that same day. *See* PE 104 (showing that the first cable downloaded was dated 1 March 2010 and that more than 250,000 cables had already been downloaded before 3 May 2010); *see also* PE 104 (proving that the "backup.xlsx" file was created on 3 May 2010). The "backup.xlsx" contained all the cables from 1 March 2010 to 30 April 2010. *See* PE 102. The accused also stored these cables from 1 March 2010 to 30 April 2010 in a file entitled "files.zip," which he transferred to his personal computer on 4 May 2010. *See* Testimony of SA Shaver; *see also* PE 127, line 57. Simply put, the accused re-introduced WGET to his SIPRNET computer after he had already stolen more than 250,000 Department of State cables.

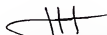
*B. The number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure.*

The number of charges and specifications do not misrepresent or exaggerate the accused's criminality, or unfairly increase the accused's punitive exposure. The combined maximum punishment for Specification 8 of Charge II and Specification 2 of Charge III, 12 years, accurately reflects the gravity and scope of the convicted offenses of adding unauthorized software to his SIPRNET computer and stealing more than 700 DABs. The combined maximum punishment for Specification 12 of Charge II and Specification 3 of Charge III, 12 years, accurately reflects the gravity and scope of the convicted offenses of stealing more than 250,000 cables, and later re-introducing unauthorized software to download another batch of cables almost one month later.


### CONCLUSION

The United States respectfully requests that the Court deny, in part, the Defense Motion. The United States agrees with the defense that Specification 16 of Charge II and Specification 4 of Charge III should merge into a single, ten-year offense for sentencing. However, for the remaining specifications which the defense requests that this Court merge, except for

Specifications 5 and 7 of Charge II which are addressed in a separate filing, the application of the *Quiroz* factors makes merger an inappropriate remedy.

  
J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 2 August 2013.

  
J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

**STIPULATION OF  
EXPECTED TESTIMONY**

**SA David Shaver**

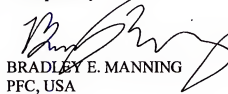
**5 August 2013**

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent David Shaver were present to testify during an Article 39(a) session of this court-martial, he would testify substantially as follows:

1. During my examination of PFC Manning's SD Card, **Prosecution Exhibit (PE) 92**, I found a file named "yada.tar.bz2.nc" and its created date was "01/30/10 10:22:19PM", as listed on **PE 105 for Identification (ID)**. I believe that PFC Manning had to create this encrypted cabinet file, similar to a "zip" file, on his Personal Mac computer, because it required specialized software. This software is "MCrypt" and I found "MCrypt" on his Personal Mac computer.
2. After decrypting the cabinet file using the password PFC Manning provided Mr. Adrian Lamo in his chats (**PE 30**), I decrypted the file. The contents of the file are listed in **PE 50 for ID**. Specifically, this file contained a file named "afg\_events.csv" with a "Last Written" date of "01/08/10 12:47:50AM" and a file named "irq\_events.csv" with a "Last Written date of "01/05/10 02:58:10AM". A cabinet file created by "MCrypt" stores each individual file's "Last Written" date within its structure, so that metadata does not change when a file is added to the cabinet or encrypted.
3. The "Last Written" date is synonymous with a Windows "Last Modified" date and essentially means that a file was last edited at that specific date or time. The "Last Written" date does not tell me whether the files were last edited on the SIPRNET or Personal Mac computer, nor does any other metadata associated with the above-referenced ".csv" files.
4. Based on my forensic analysis, the two files could have been last edited or saved on PFC Manning's SIPRNET computer or on his Personal Mac. There is no forensic data available that would indicate the exact dates PFC Manning moved or copied the files onto his Personal Mac. I know they must have been on his Personal Mac before "01/30/10 10:22:19PM" which is the creation date of the encrypted cabinet file created on his Personal Mac, and after the dates each set of data was pulled, as determined by Mr. Patrick Hoefel in paragraphs 11 and 12 of **PE 116**. I also cannot forensically determine whether the two files, containing the SIGACTS from the CIDNE-A and CIDNE-I databases, were moved or copied together or separately.

  
ASHDEN FEIN  
MAJ, JA  
Trial Counsel

  
DAVID E. COOMBS  
Civilian Defense Counsel

  
BRADLEY E. MANNING  
PFC, USA  
Accused

635  
ATTACHED  
PAGE REFERENCE  
PAGE 07 PAGES



IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE SPECIFIC  
OBJECTION UNDER R.C.M.  
1001(b)(4) FOR UNDER  
SECRETARY PATRICK  
KENNEDY**

DATED: 5 August 2013

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 1001(b)(4), requests this Court to sustain the Defense's specifically lodged objections to Under Secretary Patrick Kennedy's testimony.

STANDARD

2. A military judge's decision to admit or exclude evidence is reviewed for an abuse of discretion. *United States v. Stephens*, 67 M.J. 233, 235 (C.A.A.F. 2009).

DISCUSSION

3. The Defense specifically objected to the following testimony by Under Secretary Kennedy:

(a) The testimony related to the diminution of reporting through diplomats in the field and through those that would speak to Department of State (DOS) diplomats in various countries. Under Secretary Kennedy indicated that he believed the diminution of reporting was due to a chilling effect caused by the charged leaks in this case. The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4).

(b) The testimony related to the belief that if we (United States) do not have the trust of others, we cannot get accurate information and that if we (United States) do not get accurate information we cannot compile a complete product. The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4).

(c) The testimony related to the belief that non-governmental persons were no longer willing to talk fully and frankly with United States diplomats due to the charged leaks in this

case. The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4).

(d) The testimony related to the belief that some embassies included less information in their reporting than they did before out of fear that the information would not be protected. Under Secretary Kennedy testified that the act of reporting less information was a self-generated limitation on information from various embassies and not as a result of direction by the DOS. The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4).

(e) The testimony related to the belief that the disclosures had a chilling effect on diplomatic reporting and that the disclosures have had and will continue to have an impact on reporting for some indefinite time period. The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4) and also as being speculative.

(f) The testimony that due to the perceived chilling effect on diplomatic reporting, the decrease in information has had a negatively effect on policy makers in Washington D.C. and our interagency partners. Specifically, Under Secretary Kennedy testified that policy decisions are being made based upon incomplete information (because other countries chose not to engage in full and frank reporting, which reporting is relied on by policy makers). The Defense objects to this testimony as not be directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4) and also as being speculative. The Defense also objects based on foundation since Under Secretary Kennedy did not explain how he is familiar with policy making, the various variables that go into policy making, and how diplomatic reporting fits into policy making. Also, "policy making" is an extremely broad category. Under Secretary Kennedy did not explain what type of policy making he was referring to and certainly he is not an expert on "policy making" in general.

#### CONCLUSION

4. In light of the foregoing, the Defense requests this Court to disregard the improper testimony offered by Government through Under Secretary Kennedy.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

V.

**GOVERNMENT RESPONSE TO  
DEFENSE OBJECTION UNDER  
R.C.M 1001(b)(4)**

**5 August 2013**

(d) The testimony related to the belief that some embassies included less information in their reporting than they did before out of fear that the information would not be protected. Under Secretary Kennedy testified that the act of reporting less information was a self-generated limitation on information from various embassies and not as a result of direction by the DOS. The Defense objects to this testimony as not being directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4).

**Answer:** U/S Kennedy's opinion that Embassies included less information in their reporting was based on facts or data perceived by or made known to U/S Kennedy before the hearing. His conclusion was that PFC Manning's misconduct resulted Embassies including less information was the natural and probable consequence of PFC Manning's actions, and not based on any intervening event that played the only important part in bringing about that effect.

(e) The testimony related to the belief that the disclosures had a chilling effect on diplomatic reporting and that the disclosures have had and will continue to have an impact on reporting for some indefinite time period. The Defense objects to this testimony as not being directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4) and also as being speculative.

**Answer:** U/S Kennedy's opinion on the chilling effect on diplomatic reporting and his opinion on the future impact on reporting were based on facts or data perceived by or made known to U/S Kennedy before the hearing. His conclusion was that PFC Manning's misconduct resulted in this chilling effect and the future impact, and these results were the natural and probable consequences of PFC Manning's actions, and not based on any intervening events that played the only important part in bringing about those effects.

(f) The testimony that due to the perceived chilling effect on diplomatic reporting, the decrease in information has had a negatively effect on policy makers in Washington D.C. and our interagency partners. Specifically, Under Secretary Kennedy testified that policy decisions are being made based upon incomplete information (because other countries chose not to engage in full and frank reporting, which reporting is relied on by policy makers). The Defense objects to this testimony as not being directly related to or resulting from PFC Manning's misconduct under R.C.M. 1001(b)(4) and also as being speculative. The Defense also objects based on foundation since Under Secretary Kennedy did not explain how he is familiar with policy making, the various variables that go into policy making, and how diplomatic reporting fits into policy making. Also, "policy making" is an extremely broad category. Under Secretary Kennedy did not explain what type of policy making he was referring to and certainly he is not an expert on "policy making" in general.

**Answer:** The United States qualified U/S Kennedy as an expert in the fields of "management and operations of the Department of State" and "the use of diplomatic reporting by United States policymakers." The defense did not contest this expertise. U/S Kennedy's opinion on the impact to policy makers in Washington, DC and interagency partners was based on facts or data perceived by or made known to U/S Kennedy before the hearing, and not speculative in nature. His conclusion was that PFC Manning's misconduct had a chilling effect that negatively affected policy makers, which was the natural and probable consequence of PFC Manning's actions, and

not based on any intervening event that played the only important part in bringing about that effect.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 5 August 2013.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

UNITED STATES )

v. )

**MANNING, Bradley E., PFC** )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE WITNESS ORDER  
FOR SENTENCING**

DATED: 6 August 2013

The Defense submits the below order for the twenty-three sentencing witnesses that it intends to call in the above-captioned court-martial. The Defense no longer intends to call SGT Chad Madaras, SSG Lawrence Mitchell, or Ms. Jihreah Showman as sentencing witnesses.

**Monday, 12 August 2013**

- 1) COL David Miller
- 2) LTC Brian Kerns
- 3) MAJ Elijah Dreher
- 4) MAJ Clifford Clausen
- 5) CPT Matthew Freeburg
- 6) CPT Michael Johnson
- 7) CPT Elizabeth Fields

**Tuesday, 13 August 2013**

- 8) 1LT Tanya Gaab
- 9) CW2 Joshua Ehresman
- 10) CW2 Kyle Balonek
- 11) Mr. Paul Adkins
- 12) SGT Daniel Padgett
- 13) SGT Lorena Cooley
- 14) SGT Sheri Walsh

**Wednesday, 14 August 2013**

- 15) Ms. Lillian Smith
- 16) COL Dick Larry
- 17) CPT Michael Worsley
- 18) CAPT David Moulton
- 19) Ms. Casey Major
- 20) Ms. Debra Van Alstyne

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**RULING: Defense Motion  
For Appropriate Relief  
Under RCM 1001(b)(4)**

**5 August 2013**

---

On 31 July 2013, the Defense filed a motion to limit the Government's aggravation evidence to its proper scope under RCM 1001(b)(4) (AE 629). Specifically, the Defense objects to three categories of Government Sentencing evidence:

1. Chain of Events Testimony not directly related to the accused's charged misconduct;
2. "Could" Cause Damage Testimony; and
3. Monetary Expenses and Use of Resources Testimony

On 2 August 2013, the Government filed a response in opposition (AE 630).

**The Law:**

1. The Government may present evidence as to any aggravating circumstance directly related to or resulting from the offenses of which the accused has been found guilty. Evidence in aggravation includes, but is not limited to, evidence of financial, social, psychological, and medical impact on or cost to any person or entity who was the victim of an offense committed by the accused and evidence of significant adverse impact on the mission, discipline, or efficiency of the command directly and immediately resulting from the accused's offense. RCM 1001(b)(4) in relevant part.

2. The standard for admission of aggravating evidence under RCM 1001(b)(4) is higher than relevance. The offenses committed by the accused must have contributed to the effects that the Government proposes as aggravation. The accused's offenses must play a material role in bringing about the effects. The aggravation evidence is not admissible if an independent, intervening event played the only important part in bringing about the effect. An accused is not responsible for a never ending chain of causes and effects. *U.S. v. Rust*, 41 M.J. 472, 478 (C.A.A.F. 1995).

3. If the Court decides that evidence is proper aggravation evidence under RCM 1001(b)(4), the Court then determines whether the probative value of the aggravation evidence is substantially outweighed by the danger of unfair prejudice under MRE 403. *U.S. v. Martin*, 20 MJ 227 (C.M.A. 1985).

## INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

**USE OF FORM** - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

**COPIES** - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

**ARRANGEMENT** - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

- a. Errata sheet, if any.
- b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
- c. Record of proceedings in court, including Article 39(a) sessions, if any.
- d. Authentication sheet, followed by certificate of correction, if any.
- e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
- f. Exhibits admitted in evidence.
- g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
- h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.